Guide du développeur

AWS Config

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: Guide du développeur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que c'est AWS Config ? ... 1
Considérations ... 1
Moyens d'utilisation AWS Config ... 1
Gestion des ressources ... 2
Audit et conformité ... 2
Gestion et résolution des problèmes de changements de configuration ... 2
Analyse de sécurité ... 2
Solutions partenaires ... 3
Fonctionnalités ... 3
Comment AWS Config fonctionne ... 4
Découverte de ressources ... 5
Suivi des ressources ... 5
Livraison des éléments de configuration ... 6
Contrôlez l'accès à AWS Config ... 10
Concepts ... 10
AWS Config Interfaces ... 11
Gestion des ressources ... 12
Enregistreur de configuration ... 13
Canal de livraison ... 6
AWS Config Règles ... 15
Packs de conformité ... 18
Agrégateurs ... 19
Prise en charge de la région ... 20
Service Limits ... 25
AWS Intégrations de services ... 27
AWS Organizations ... 27
AWS Control Tower ... 27
AWS CloudTrail ... 27
AWS Security Hub ... 28
AWS Audit Manager ... 28
AWS Systems Manager ... 28
AWS Firewall Manager ... 29
Hôtes dédiés Amazon EC2 ... 29
Application Load Balancers ... 30

AWS CodeBuild ... 30
AWS X-Ray ... 30
Connecteur AWS Service Management ... 30
Amazon API Gateway ... 30
Informations supplémentaires ... 31
AWS Kits de développement logiciel pour AWS Config ... 32
Démarrage ... 34
S'inscrire à AWS ... 34
Inscrivez-vous pour un Compte AWS ... 34
Création d'un utilisateur doté d'un accès administratif ... 35
Façons de démarrer avec AWS Config ... 36
Configuration AWS Config (console) ... 36
Configuration ... 36
Configuration en un clic ... 37
Configuration manuelle ... 41
Configuration AWS Config (AWS CLI) ... 48
Configuration ... 49
Prérequis ... 49
Démarrage AWS Config ... 113
Vérification ... 124
Utilisation des AWS SDK ... 126
Enregistreur de configuration ... 128
Gestion de l'enregistreur de configuration (console) ... 128
Gestion de l'enregistreur de configuration (AWS CLI) ... 129
Détection des dérives de l'enregistreur de configuration ... 133
Canal de livraison ... 134
Terminologie ... 135
Mise à jour du canal de livraison ... 136
Renommer les canaux de livraison ... 140
Composants d'un élément de configuration ... 141
Diffusion d'un instantané de la configuration ... 143
Fourniture d'instantanés de configuration ... 143
Exemple de capture instantanée de configuration à partir de AWS Config ... 144
Vérification de l'état de diffusion ... 149
Affichage de l'instantané de configuration dans un compartiment Amazon S3 ... 150
Exemples de notifications ... 151

Exemple de notification de changement d'élément de configuration 152
Exemple de notification de diffusion de l'historique de configuration 167
Exemple de notification de démarrage de la diffusion d'un instantané de configuration 168
Exemple de notification de diffusion d'un instantané de configuration 169
Exemple de notification de modification de conformité 170
Exemple de notification d'une évaluation de règles démarrée 173
Exemple de notification de changement avec un élément de configuration trop grand 174
Exemple de notification d'échec de diffusion 176
Gestion des ressources 178
AWS Config Tableau de bord 179
Conformité et inventaire des ressources 179
AWS Config Indicateurs d'utilisation et de réussite 181
Types de ressource pris en charge 184
Amazon AppStream 185
Amazon AppFlow 185
..... 185
Amazon API Gateway 186
Amazon Athena 186
Amazon CloudFront 187
Amazon CloudWatch 188
Amazon CodeGuru 188
Amazon Cognito 189
Amazon Connect 189
Amazon Detective 190
Amazon DynamoDB 190
Amazon EC2 191
Amazon ECR 198
Amazon ECS 199
Amazon EFS 200
Amazon EKS 200
Amazon EMR 201
Amazon EventBridge 201
Amazon Forecast 202
Amazon Fraud Detector 202
Amazon GuardDuty 203
Amazon Inspector 204

Amazon IVS 204
Amazon Keyspaces 204
Amazon OpenSearch Service 205
Amazon Personalize 206
Amazon Pinpoint 206
Amazon QLDB 207
Amazon Kendra 208
Amazon Kinesis 208
Amazon Lex 209
Amazon Lightsail 209
Amazon Lookout for Metrics 210
Amazon Lookout for Vision 210
Amazon Managed Grafana 210
Amazon Managed Service for Prometheus 211
Amazon MemoryDB for Redis 211
Amazon MQ 211
Amazon MSK 211
Amazon Redshift 212
Amazon RDS 214
Amazon Route 53 215
Amazon SageMaker 217
Amazon SES 218
Amazon SNS 219
Amazon SQS 219
Amazon S3 219
Amazon WorkSpaces 221
AWS Amplify 222
AWS AppConfig 222
AWS App Runner 223
AWS App Mesh 223
AWS AppSync 224
AWS Audit Manager 225
AWS Auto Scaling 225
AWS Backup 226
AWS Batch 227
AWS Budgets 227

AWS Certificate Manager 228
AWS CloudFormation 228
AWS CloudTrail 228
AWS Cloud9 229
AWS Cloud Map 229
AWS CodeArtifact 230
AWS CodeBuild 230
AWS CodeDeploy 230
AWS CodePipeline 231
AWS Config 232
AWS DMS 233
AWS DataSync 233
AWS Device Farm 235
AWS Elastic Beanstalk 235
AWS FIS 236
AWS Global Accelerator 236
AWS Glue 237
AWS Ground Station 237
AWS HealthLake 238
AWS IAM 238
AWS IoT 239
AWS KMS 243
AWS Lambda 243
AWS Mainframe Modernization 244
AWS Network Firewall 244
AWS Network Manager 245
AWS Panorama 246
AWS Private CA 247
AWS Resilience Hub 247
Explorateur de ressources AWS 248
AWS RoboMaker 248
AWS Signer 249
AWS Secrets Manager 249
AWS Service Catalog 249
AWS Shield 250
AWS Step Functions 250

AWS Systems Manager ... 251
AWS Transfer Family ... 252
AWS WAF ... 252
AWS X-Ray ... 254
Elastic Load Balancing ... 255
MediaConnect ... 256
MediaPackage ... 256
MediaTailor ... 257
Couverture des ressources en fonction de la disponibilité dans les régions ... 257
Amérique du Nord et du Sud ... 257
Europe ... 318
Asie-Pacifique ... 366
Chine ... 414
Afrique et Moyen-Orient ... 448
GovCloud ... 496
AWS Ressources d'enregistrement ... 540
Considérations ... 540
Ressources régionales et mondiales ... 541
Enregistrement de ressources (console) ... 545
Ressources d'enregistrement (AWS CLI) ... 549
Fréquence d’enregistrement ... 565
Arrêt de l’enregistrement ... 566
Ressources non enregistrées ... 566
AWS Config Règles et types de ressources globaux ... 567
Enregistrement de ressources tierces ... 569
Étape 1 : Configurer votre environnement de développement ... 570
Étape 2 : Modéliser votre ressource ... 570
Étape 3 : Générer des artefacts ... 572
Étape 4 : Enregistrer la ressource ... 572
Étape 5 : Publier la configuration des ressources ... 573
Enregistrer et supprimer un état de configuration pour des ressources tierces à l'aide de AWS CLI ... 573
Gestion d'un état de configuration pour le type de ressources tierces à l'aide d'API ... 576
Configurations du logiciel d'enregistrement ... 576
Afficher les ressources enregistrées ... 579
Inventaire des ressources ... 580

Informations sur la conformité et résultats de l'évaluation ... 582
Historique de configuration et de conformité ... 595
Balisage de vos ressources ... 604
Restrictions liées au balisage ... 604
Gestion des balises à l'aide des actions d'API AWS Config ... 605
AWS Règles de configuration ... 606
Considérations de coût ... 607
Prise en charge de la région ... 608
Composants d'une règle ... 615
Métadonnées de règles ... 615
Structure des règles ... 617
Mode d'évaluation ... 636
Types de déclencheurs ... 636
Modes d'évaluation ... 638
Évaluations des règles ... 642
Règles gérées ... 642
Considérations de coût ... 607
Types de déclencheurs ... 643
Modes d'évaluation ... 645
Liste des règles gérées ... 646
Liste des règles gérées par mode d'évaluation ... 949
Liste des règles gérées par type de déclencheur ... 965
Liste des règles gérées en fonction de la disponibilité dans les régions ... 980
Règles liées à un service ... 1317
Création de règles gérées à l'aideAWS CloudFormation de modèles ... 1318
Règles personnalisées ... 1320
Règles de politiques personnalisées ... 1320
Règles Lambda personnalisées ... 1320
Considérations de coût ... 607
Types de déclencheurs ... 1322
Modes d'évaluation ... 1323
Gestion des ressources supprimées ... 1324
Création de règles de politiques personnalisées ... 1326
Création de règles Lambda personnalisées ... 1330
Ajout, mise à jour et suppression de règles ... 1364
Utilisation de la console ... 1364

Utilisation des AWS SDK ... 1371
Utilisation de Security Hub ... 1383
Évaluation des ressources à l'aide de règles ... 1383
Suppression des résultats de l'évaluation ... 1388
Supprimer les résultats de l'évaluation (console) ... 1388
Suppression des résultats d'évaluation (CLI) ... 1389
Suppression des résultats d'évaluation (API) ... 1389
Gestion des règles organisationnelles ... 1389
Considérations ... 1390
Déploiement ... 1391
Prise en charge de la région ... 1391
Correction ... 1394
Prérequis ... 1395
Configuration de la correction manuelle (console) ... 1395
Configuration de la correction automatique (console) ... 1396
Suppression d’une action de correction (console) ... 1398
Gestion de correction (API) ... 1398
Prise en charge de la région ... 1399
Résolution des problèmes ... 1403
Packs de conformité ... 1406
Prérequis ... 1406
Commencer AWS Config l'enregistrement ... 1407
Conditions préalables à l'utilisation d'un pack de conformité avec la correction ... 1407
Conditions préalables à l'utilisation d'un pack de conformité avec une ou plusieurs règles AWS Config ... 1408
Conditions préalables pour les packs de conformité d'organisation ... 1411
Prise en charge de la région ... 1412
Vérifications des processus ... 1417
Exemple de modèle de pack de conformité pour créer des vérifications de processus ... 1418
Comprend Process Checks Within a Conformance Pack ... 1419
Modifier le statut de conformité d'une vérification de processus ... 1420
Afficher et modifier la vérification du processus (Console) ... 1421
Exemples de modèles de pack de conformité ... 1421
AWSPack de conformité pour garde-corps Control Tower Detective ... 1426
Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Material . 1426
Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Standard 1682

Bonnes pratiques de fonctionnement pour ACSC Essentials 8 1869
Bonnes pratiques de fonctionnement pour ACSC ISM 1898
Bonnes pratiques de fonctionnement pour l'IA et le ML 2054
Bonnes pratiques de fonctionnement pour Amazon API Gateway 2055
Bonnes pratiques opérationnelles pour Amazon CloudWatch 2055
Bonnes pratiques opérationnelles pour Amazon DynamoDB 2055
Bonnes pratiques opérationnelles pour Amazon S3 2055
Bonnes pratiques de fonctionnement pour APRA CPG 234 2055
Bonnes pratiques de fonctionnement pour la gestion des ressources 2312
Bonnes pratiques de fonctionnement pour AWS Backup 2312
Bonnes pratiques opérationnelles pour la gestion des AWS identités et des accès 2313
Meilleures pratiques opérationnelles pour le pilier de fiabilité du AWS framework Well-Architected 2313
Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected 2388
Bonnes pratiques de fonctionnement pour le BCP et la DR 2589
Bonnes pratiques de fonctionnement pour BNM RMiT 2590
Bonnes pratiques de fonctionnement pour le profil moyen de contrôle du cloud du Canadian Centre for Cyber Security (CCCS) 2939
Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 1 4699
Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 2 4744
Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG1 .. 4803
Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG2 .. 4915
Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG3 .. 5111
Bonnes pratiques de fonctionnement pour CIS Top 20 5325
Bonnes pratiques de fonctionnement pour CISA Cyber Essentials 5415
Bonnes pratiques de fonctionnement pour la division Criminal Justice Information Services (CJIS) 5654
Bonnes pratiques de fonctionnement pour CMMC niveau 1 5805
Bonnes pratiques de fonctionnement pour CMMC niveau 2 5947
Bonnes pratiques de fonctionnement pour CMMC niveau 3 6302
Bonnes pratiques de fonctionnement pour CMMC niveau 4 6823
Bonnes pratiques de fonctionnement pour CMMC niveau 5 7388
Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 1 8027

Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 2 8167
Bonnes pratiques de fonctionnement pour les services de calcul 8651
Bonnes pratiques de fonctionnement pour la résilience des données 8651
Bonnes pratiques de fonctionnement pour les services de base de données 8651
Bonnes pratiques de fonctionnement pour les services de lac de données et d'analyse 8651
Bonnes pratiques de fonctionnement pour DevOps 8652
Bonnes pratiques de fonctionnement pour EC2 8652
Bonnes pratiques de fonctionnement pour les services de chiffrement et de gestion des clés 8652
Bonnes pratiques de fonctionnement pour le guide de la cybersécurité pour les PME de l'ENISA 8653
Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau faible) 8880
Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau modéré) 9001
Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau élevé) 9138
Bonnes pratiques de fonctionnement pour la norme FDA CFR Titre 21 Partie 11 9284
Bonnes pratiques de fonctionnement pour FedRAMP(Low) 9703
Bonnes pratiques de fonctionnement pour FedRAMP (modérée) 10017
Bonnes pratiques de fonctionnement pour FFIEC 10659
Bonnes pratiques de fonctionnement pour Germany Cloud Computing Compliance Criteria Catalog (C5) 10921
Bonnes pratiques de fonctionnement pour Gramm Leach Bliley Act (GLBA) 11020
Bonnes pratiques de fonctionnement pour GxP EU Annex 11 11082
Bonnes pratiques de fonctionnement pour la sécurité HIPAA 11264
Bonnes pratiques de fonctionnement pour IRS 1#075 11826
Bonnes pratiques de fonctionnement pour K-ISMS 12074
Bonnes pratiques de fonctionnement pour l'équilibrage de charge 12174
Bonnes pratiques de fonctionnement pour la journalisation 12174
Bonnes pratiques de fonctionnement pour les services de gestion et de gouvernance 12174
Bonnes pratiques de fonctionnement pour MAS Notice 655 12174
Bonnes pratiques de fonctionnement pour MAS TRMG 12219
Bonnes pratiques de fonctionnement pour la surveillance 12484
Bonnes pratiques de fonctionnement pour NBC TRMG 12484
Bonnes pratiques de fonctionnement pour NERC CIP BCSI 13084
Bonnes pratiques de fonctionnement pour les principes de sécurité du cloud NCSC 13157
Bonnes pratiques de fonctionnement pour NCSC Cyber Assesment Framework 13287

Bonnes pratiques de fonctionnement pour les services de mise en réseau et de diffusion de contenu 13503
Bonnes pratiques de fonctionnement pour NIST 800-53 rev 4 13503
Bonnes pratiques de fonctionnement pour NIST 800-53 rev 5 13873
Bonnes pratiques de fonctionnement pour NIST 800 171 14794
Bonnes pratiques de fonctionnement pour NIST 800 172 15194
Bonnes pratiques de fonctionnement pour NIST 800 181 15280
Bonnes pratiques de fonctionnement pour NIST 1800 25 15889
Bonnes pratiques de fonctionnement pour NIST CSF 16083
Bonnes pratiques de fonctionnement pour le cadre de confidentialité NIST v1.0 16518
Bonnes pratiques de fonctionnement pour NYDFS 23 16808
Bonnes pratiques de fonctionnement pour NZISM 17031
Bonnes pratiques de fonctionnement pour PCI DSS 3.2.1 17130
Bonnes pratiques de fonctionnement pour les ressources accessibles au public 17594
Bonnes pratiques de fonctionnement pour le cadre de cybersécurité RBI pour les UCB ... 17595
Bonnes pratiques de fonctionnement pour RBI MD-ITF 17652
Bonnes pratiques de fonctionnement pour les services de sécurité, d'identité et de conformité 17825
Bonnes pratiques de fonctionnement pour le sans serveur 17825
Bonnes pratiques de fonctionnement pour les services de stockage 17825
Bonnes pratiques de fonctionnement pour SWIFT CSP 17826
Bonnes pratiques de sécurité pour Amazon Elastic Container Service (Amazon ECS) 17866
Bonnes pratiques de sécurité pour Amazon Elastic File System (Amazon EFS) 17867
Bonnes pratiques de sécurité pour Amazon Elastic Kubernetes Service (Amazon EKS) .. 17867
Bonnes pratiques en matière de sécurité pour Amazon CloudFront 17867
Bonnes pratiques en matière de sécurité pour Amazon OpenSearch Service 17867
Bonnes pratiques de sécurité pour Amazon Redshift 17868
Bonnes pratiques de sécurité pour Amazon Relational Database Service (Amazon RDS) 17868
Bonnes pratiques de sécurité pour AWS Auto Scaling 17868
Bonnes pratiques de sécurité pour AWS CloudTrail 17869
Bonnes pratiques de sécurité pour AWS CodeBuild 17869
Bonnes pratiques de sécurité pour Amazon ECR 17869
Bonnes pratiques de sécurité pour AWS Lambda 17869
Bonnes pratiques de sécurité pour AWS Network Firewall 17870
Bonnes pratiques en matière de sécurité pour Amazon SageMaker 17870
Bonnes pratiques de sécurité pour AWS Secrets Manager 17870

Bonnes pratiques de sécurité pour AWS WAF 17870
Exemples de modèle avec action de correction 17871
Packs de conformité personnalisés 17871
Terminologie 17871
Personnalisation du modèle 17872
Déploiement de votre pack de conformité personnalisé 17876
Tableau de bord du pack de conformité 17877
Navigation sur la page principale des packs de conformité 17877
En savoir plus 17878
Affichage de l'historique de conformité 17878
Affichage de la chronologie de conformité 17879
Interrogation de l'historique de conformité 17880
Déploiement d'un pack de conformité (console) 17881
Déploiement d'un pack de conformité à l'aide de modèles 17882
Modifier un pack de conformité 17883
Supprimer un pack de conformité 17884
Déploiement d'un pack de conformité (AWS CLI) 17884
Déployer un pack de conformité 17885
Afficher un pack de conformité 17886
Afficher l'état du pack de conformité 17887
Afficher l'état de conformité du pack de conformité 17887
Obtenir les détails de conformité pour un pack de conformité spécifique 17888
Supprimer un pack de conformité 17889
Gestion des packs de conformité (API) 17889
Gestion des packs de conformité d'une organisation 17890
Considérations 17890
Déploiement 17891
Prise en charge de la région 17892
Résolution des problèmes 17894
État d'échec d'un pack de conformité 17894
Des règles en suspens dans un pack de conformité 17896
Agrégateurs 17898
Cas d'utilisation 17898
Terminologie 17899
Comment agréger les données 17899
Prise en charge de la région 17900

Résolution des problèmes 17904
Tableau de bord Agrégateur 17906
Utilisation du tableau de bord Agrégateur 17906
Tableau de bord de conformité 17909
Tableau de bord d'inventaire 17912
Configuration d'un agrégateur (console) 17914
Créer un agrégateur 17914
Modification d'un agrégateur 17917
Suppression d'un agrégateur 17917
Configuration d'un agrégateur (AWS CLI) 17917
Ajout d'un agrégateur à l'aide de comptes individuels 17918
Ajout d'un agrégateur à l'aide d' AWS Organizations 17919
Enregistrer un administrateur délégué 17921
Affichage d'un agrégateur 17923
Modification d'un agrégateur 17924
Suppression d'un agrégateur 17926
Autorisation des comptes Aggregator (console) 17926
Considérations 17926
Ajout d'une autorisation pour des comptes et des régions Aggregator 17927
Autorisation d'une demande en attente pour un compte Aggregator 17928
Suppression d'une autorisation pour un compte Aggregator existant 17928
Autorisation des comptes Aggregator (AWS CLI) 17929
Considérations 17929
Ajout d'une autorisation pour des comptes et des régions Aggregator 17930
Suppression d'un compte d'autorisation 17930
Requêtes avancées 17931
Fonctionnalités 17932
Composants d'une requête 17932
Résumé 17932
Paramètres 17933
Exemples 17933
Exemples de requêtes 17933
Exemples de requêtes relationnelles 17939
Limites 17941
Prise en charge de la région 17944
Éditeur de requête (Console) 17948

Considérations 17948
Utiliser un AWS exemple de requête 17948
Création de votre requête personnalisée 17949
Éditeur de requête (AWS CLI) 17950
Considérations 17950
Interrogation des données de configuration des ressources 17951
Enregistrement d'une requête 17953
Affichage de toutes les requêtes enregistrées 17954
Obtention des détails d'une requête enregistrée 17954
Suppression d'une requête enregistrée 17955
Processeur de requêtes en langage naturel 17955
Considérations 17955
Requête à l’aide du processeur de requêtes en langage naturel 17948
Exemples d'instructions 17957
Fournir des commentaires 17960
Prise en charge de la région 17961
Suppression des données 17962
Définition de la période de conservation des données (console) 17964
Sécurité 17966
Protection des données 17967
Chiffrement des données en transit 17968
Chiffrement des données en transit 17968
Gestion de l’identité et des accès 17968
Public ciblé 17969
Authentification par des identités 17969
Gestion des accès à l’aide de politiques 17973
Comment AWS Config fonctionne avec IAM 17976
Exemples de politiques basées sur l’identité 17984
AWS politiques gérées 18003
Autorisations du rôle IAM 18153
Mise à jour du rôle IAM 18157
Autorisations pour le compartiment Amazon S3 18158
Autorisations pour la clé KMS 18163
Autorisations relatives à la rubrique Amazon SNS 18166
Résolution des problèmes 18170
Utilisation des rôles liés à un service 18172

Réponse aux incidents 18174
Validation de la conformité 18175
Résilience 18176
Sécurité de l'infrastructure 18177
Configuration et analyse des vulnérabilités 18177
Prévention du cas de figure de l'adjoint désorienté entre services 18178
Bonnes pratiques 18178
Journalisation et surveillance 18180
Journalisation 18180
AWS Config Informations dans CloudTrail 18180
Comprendre les entrées du fichier AWS Config journal 18182
Exemples de fichiers journaux 18182
Surveillance 18190
Utilisation d'Amazon SQS 18190
Utilisation d'Amazon EventBridge 18192
Points de terminaison Amazon VPC 18198
Créez un point de terminaison VPC pour AWS Config 18198
FAQ 18199
Impossible de voir mes dernières modifications de configuration 18199
Puis-je m'attendre à voir mes modifications de configuration immédiatement ? 18199
Relations indirectes dans AWS Config 18199
Qu'est-ce que la relation entre les ressources ? 18199
Que sont les relations directes et indirectes entre les ressources ? 18200
Quelles sont les relations indirectes prises AWS Config en charge ? 18200
Comment les éléments de configuration sont-ils créés en cas de relation directe et indirecte ? 18202
Quels sont les éléments de configuration générés par les relations indirectes ? 18202
Comment récupérer les données de configuration liées aux relations indirectes ? 18204
Exemples de code 18206
Actions 18207
`DeleteConfigRule` 18207
`DescribeComplianceByConfigRule` 18209
`DescribeComplianceByResource` 18211
`DescribeConfigRuleEvaluationStatus` 18213
`DescribeConfigRules` 18215
`DescribeConfigurationRecorderStatus` 18218

`DescribeConfigurationRecorders` 18220
`DescribeDeliveryChannels` 18221
`GetComplianceDetailsByConfigRule` 18222
`GetComplianceDetailsByResource` 18225
`GetComplianceSummaryByConfigRule` 18227
`GetComplianceSummaryByResourceType` 18228
`PutConfigRule` 18231
`PutDeliveryChannel` 18234
Historique du document 18237
Mises à jour antérieures 18362
..... 18434

Qu'est-ce que c'est AWS Config ?

AWS Config fournit une vue détaillée de la configuration des AWS ressources de votre AWS compte. Elle indique comment les ressources sont liées entre elles et comment elles ont été configurées dans le passé, pour que vous puissiez observer comment les configurations et les relations changent au fil du temps.

Une AWS ressource est une entité avec laquelle vous pouvez travailler AWS, telle qu'une instance Amazon Elastic Compute Cloud (EC2), un volume Amazon Elastic Block Store (EBS), un groupe de sécurité ou un Amazon Virtual Private Cloud (VPC). Pour une liste complète des AWS ressources prises en charge par AWS Config, voirTypes de ressource pris en charge.

Considérations

- Compte AWS: Vous avez besoin d'un actif Compte AWS. Pour plus d'informations, consultez la section Inscription à AWS.
- Compartiment Amazon S3 : vous avez besoin d'un compartiment S3 pour recevoir les données relatives à vos instantanés de configuration et à votre historique. Pour de plus d'informations, consultez Autorisations pour le compartiment Amazon S3.
- Rubrique Amazon SNS : vous avez besoin d'un Amazon SNS pour recevoir des notifications lorsque des modifications sont apportées à vos instantanés de configuration et à votre historique. Pour plus d'informations, consultez la rubrique Autorisations pour Amazon SNS.
- Rôle IAM : vous avez besoin d'un rôle IAM disposant des autorisations d'accès nécessaires. AWS Config Pour plus d'informations, consultez la section Autorisations pour le rôle IAM.
- Types de ressources : vous pouvez décider quels types de ressources vous AWS Config souhaitez enregistrer. Pour plus d'informations, consultez la section AWS Ressources d'enregistrement.

Moyens d'utilisation AWS Config

Lorsque vous exécutez vos applications AWS, vous utilisez généralement AWS des ressources que vous devez créer et gérer collectivement. La demande pour votre application ne cesse de croître, tout comme votre besoin de suivre vos AWS ressources. AWS Config est conçu pour vous aider à superviser les ressources de votre application dans les scénarios suivants :

Gestion des ressources

Pour gérer au mieux les configurations de vos ressources et détecter les erreurs de configuration de ressources, vous devez avoir, à tout moment, une visibilité précise de vos ressources existantes et de leur configuration. Vous pouvez l'utiliser AWS Config pour vous avertir chaque fois que des ressources sont créées, modifiées ou supprimées sans avoir à surveiller ces modifications en interrogeant les appels passés à chaque ressource.

Vous pouvez utiliser AWS Config des règles pour évaluer les paramètres de configuration de vos AWS ressources. Lorsqu'il AWS Config détecte qu'une ressource enfreint les conditions de l'une de vos règles, AWS Config signale la ressource comme non conforme et envoie une notification. AWS Config évalue en permanence vos ressources au fur et à mesure de leur création, de leur modification ou de leur suppression.

Audit et conformité

Vous pourriez utiliser les données qui nécessitent des audits fréquents afin de garantir la conformité avec les stratégies internes et les bonnes pratiques. Pour illustrer la conformité, vous devez accéder à l'historique de configuration de vos ressources. Ces informations sont fournies par AWS Config.

Gestion et résolution des problèmes de changements de configuration

Lorsque vous utilisez plusieurs AWS ressources qui dépendent les unes des autres, une modification de la configuration d'une ressource peut avoir des conséquences imprévues sur les ressources associées. Vous pouvez ainsi voir comment la ressource que vous souhaitez modifier est liée aux autres ressources et évaluer l'impact de votre modification. AWS Config

Vous pouvez également utiliser l'historique des configurations de vos ressources fournies par AWS Config pour résoudre des problèmes et pour accéder à la dernière configuration correcte connue d'une ressource posant problème.

Analyse de sécurité

Pour analyser les failles de sécurité potentielles, vous avez besoin d'informations historiques détaillées sur les configurations de vos AWS ressources, telles que les autorisations AWS Identity and Access Management (IAM) accordées à vos utilisateurs ou les règles du groupe de sécurité Amazon EC2 qui contrôlent l'accès à vos ressources.

Vous pouvez l'utiliser AWS Config pour consulter la politique IAM attribuée à un utilisateur, à un groupe ou à un rôle à tout moment pendant AWS Config l'enregistrement. Ces données peuvent

vous aider à identifier les autorisations qui appartenaient à un utilisateur à un moment précis : par exemple, vous pouvez voir si l'utilisateur `John Doe` disposait d'une autorisation pour modifier les paramètres Amazon VPC le 1er janvier 2015.

Vous pouvez également l'utiliser AWS Config pour afficher la configuration de vos groupes de sécurité EC2, y compris les règles de port ouvertes à un moment précis. Ces informations peuvent vous aider à déterminer si un groupe de sécurité a bloqué le trafic TCP entrant dans un port spécifique.

Solutions partenaires

AWS s'associe à des spécialistes tiers en journalisation et en analyse pour fournir des solutions qui utilisent les AWS Config résultats. Pour plus d'informations, consultez la page AWS Config détaillée à l'adresse AWS Config.

Fonctionnalités

Lors de la configuration AWS Config, vous pouvez effectuer les opérations suivantes :

Gestion des ressources

- Spécifiez les types de ressources que vous AWS Config souhaitez enregistrer.

- Configurez un compartiment Amazon S3 pour recevoir un instantané de configuration sur demande et un historique de configuration.
- Configurez Amazon SNS pour envoyer des notifications de diffusion de configuration.
- Accordez-lui AWS Config les autorisations nécessaires pour accéder au compartiment Amazon S3 et à la rubrique Amazon SNS.

  Pour plus d'informations, consultez les sections Affichage AWS des configurations et de l'historique des AWS ressources et Gestion des configurations et de l'historique des ressources.

Règles et packs de conformité

- Spécifiez les règles que vous souhaitez utiliser AWS Config pour évaluer les informations de conformité pour les types de ressources enregistrés.
- Utilisez des packs de conformité ou un ensemble de AWS Config règles et d'actions correctives qui peuvent être déployées et surveillées en tant qu'entité unique dans votre. Compte AWS

Pour plus d'informations, consultez la section Évaluation des ressources à l'aide de AWS Config règles et de packs de conformité.

Agrégateurs

- Utilisez un agrégateur pour obtenir une vue centralisée de votre inventaire de ressources et de votre conformité. Un agrégateur collecte les données AWS Config de configuration et de conformité provenant de plusieurs AWS régions au Comptes AWS sein d'un seul compte et d'une seule région.

  Pour plus d'informations, consultez Regroupement des données de plusieurs comptes et plusieurs régions.

Requêtes avancées

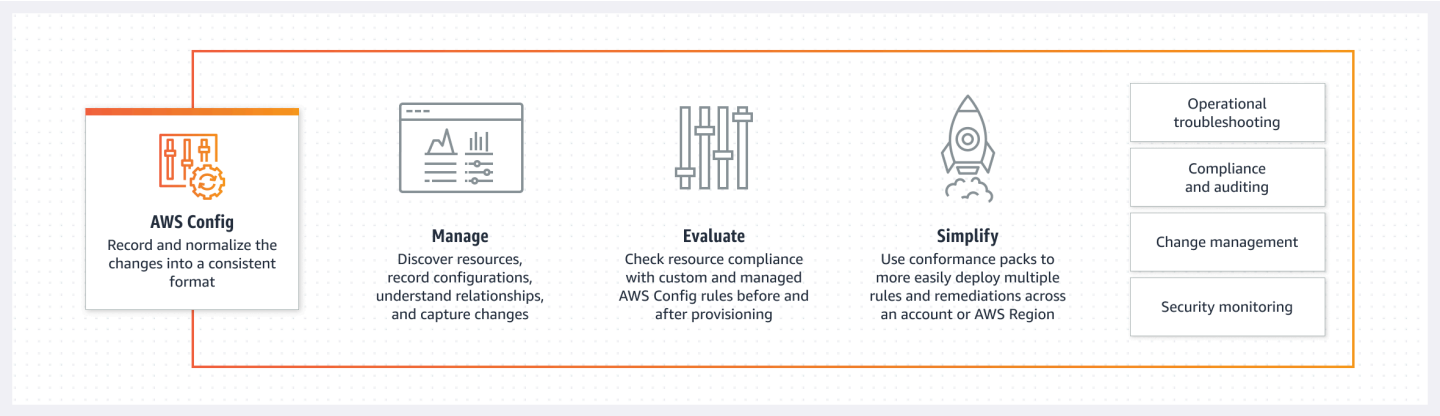
- Utilisez l'un des exemples de requêtes ou rédigez votre propre requête en vous référant au schéma de configuration de la AWS ressource.

  Pour plus d'informations, consultez la section Interrogation de l'état de configuration actuel des AWS ressources.

Comment AWS Config fonctionne

AWS Config fournit une vue détaillée de la configuration des AWS ressources de votre AWS compte. Elle indique comment les ressources sont liées entre elles et comment elles ont été configurées dans le passé, pour que vous puissiez observer comment les configurations et les relations changent au fil du temps.

Une AWS ressource est une entité avec laquelle vous pouvez travailler AWS, telle qu'une instance Amazon Elastic Compute Cloud (EC2), un volume Amazon Elastic Block Store (EBS), un groupe de sécurité ou un Amazon Virtual Private Cloud (VPC). Pour une liste complète des AWS ressources prises en charge par AWS Config, voirTypes de ressource pris en charge.



Découverte de ressources

Lorsque vous l'activez AWS Config, il découvre d'abord les AWS ressources prises en charge qui existent dans votre compte et génère un élément de configuration pour chaque ressource.

AWS Config génère également des éléments de configuration lorsque la configuration d'une ressource change, et il conserve des enregistrements historiques des éléments de configuration de vos ressources depuis le démarrage de l'enregistreur de configuration. Par défaut, AWS Config crée des éléments de configuration pour chaque ressource prise en charge dans la région. Si vous ne souhaitez pas AWS Config créer d'éléments de configuration pour toutes les ressources prises en charge, vous pouvez spécifier les types de ressources que vous souhaitez suivre.

Avant de spécifier un type de ressource AWS Config à suivre, vérifiez la couverture des ressources par région disponible pour voir si le type de ressource est pris en charge dans la AWS région dans laquelle vous configurez AWS Config. Si un type de ressource est pris AWS Config en charge par au moins une région, vous pouvez activer l'enregistrement de ce type de ressource dans toutes les régions prises en charge par AWS Config, même si le type de ressource spécifié n'est pas pris en charge par la AWS région dans laquelle vous configurez AWS Config.

Suivi des ressources

AWS Config assure le suivi de toutes les modifications apportées à vos ressources en appelant l'appel d'API Describe ou List pour chaque ressource de votre compte. Le service utilise les appels d'interfaces API pour capturer les détails de configuration de toutes les ressources connexes.

Par exemple, la suppression d'une règle de sortie d'un groupe de sécurité VPC AWS Config entraîne l'appel d'un appel d'API Describe sur le groupe de sécurité. AWS Config invoque ensuite un appel d'API Describe sur toutes les instances associées au groupe de sécurité. Les configurations mises

à jour du groupe de sécurité (la ressource) et de chaque instance (les ressources connexes) sont enregistrées comme éléments de configuration et sont diffusées dans un flux de configuration vers un compartiment Amazon Simple Storage Service (Amazon S3).

AWS Config suit également les modifications de configuration qui n'ont pas été initiées par l'API. AWS Config examine régulièrement les configurations des ressources et génère des éléments de configuration pour les configurations modifiées.

Si vous utilisez des AWS Config règles, évalue AWS Config en permanence les configurations de vos AWS ressources pour déterminer les paramètres souhaités. Selon la règle, AWS Config évaluera vos ressources soit en réponse aux modifications de configuration, soit périodiquement. Chaque règle est associée à une fonction AWS Lambda qui contient la logique d'évaluation de la règle. Lors de AWS Config l'évaluation de vos ressources, il invoque la fonction de la règle. AWS Lambda La fonction renvoie l'état de conformité des ressources évaluées. Si une ressource enfreint les conditions d'une règle, AWS Config signale la ressource et la règle comme non conformes. Lorsque le statut de conformité d'une ressource change, AWS Config envoie une notification à votre rubrique Amazon SNS.

Livraison des éléments de configuration

AWS Config peut fournir des éléments de configuration via l'un des canaux suivants :

Compartiment Amazon S3

AWS Config suit les modifications apportées à la configuration de vos AWS ressources et envoie régulièrement des informations de configuration mises à jour à un compartiment Amazon S3 que vous spécifiez. Pour chaque type de ressource qui AWS Config enregistre, il envoie un fichier d'historique de configuration toutes les six heures. Chaque fichier historique de configuration contient des détails sur les ressources qui ont été modifiées au cours de cette période de six heures. Chaque fichier comprend des ressources d'un seul type, par exemple les instances Amazon EC2 ou les volumes Amazon EBS. Si aucune modification de configuration ne se produit, AWS Config n'envoie pas de fichier.

AWS Config envoie un instantané de configuration à votre compartiment Amazon S3 lorsque vous utilisez la commande deliver-config-snapshot avec la AWS CLI ou lorsque vous utilisez l'action DeliverConfigSnapshot avec l'API. AWS Config Un instantané de configuration contient les détails de configuration de toutes les ressources AWS Config enregistrées dans votre Compte AWS. Le fichier historique de configuration et l'instantané de la configuration sont au format JSON.

> **Note**
>
> AWS Config fournit uniquement les fichiers d'historique de configuration et les instantanés de configuration au compartiment S3 spécifié ; AWS Config ne modifie pas les politiques de cycle de vie des objets du compartiment S3. Vous pouvez utiliser des politiques de cycle de vie pour spécifier si vous souhaitez supprimer ou archiver les objets dans Amazon S3 Glacier. Pour plus d'informations, consultez Gestion de la configuration du cycle de vie dans le Guide de l'utilisateur Amazon Simple Storage Service. Vous pouvez aussi consulter le billet de blog relatif à l'archivage des données Amazon S3 dans S3 Glacier.

Rubrique Amazon SNS

Une rubrique Amazon Simple Notification Service (Amazon SNS) est un canal de communication utilisé par Amazon SNS pour envoyer des messages (ou des notifications) aux points de terminaison d'abonnement tels qu'une adresse e-mail ou des clients. D'autres types de notifications Amazon SNS comprennent les notifications push liées aux applications de téléphones mobiles, les notifications SMS sur des smartphones ou des téléphones mobiles pouvant recevoir des SMS, ainsi que les requêtes HTTP POST. Pour obtenir de meilleurs résultats, utilisez Amazon SQS comme point de terminaison de notification pour la rubrique SNS, puis traitez les informations contenues dans la notification par programmation.

AWS Config utilise la rubrique Amazon SNS que vous spécifiez pour vous envoyer des notifications. Le type de notification que vous recevez est indiqué par la valeur pour la clé `messageType` dans le corps du message, comme dans l'exemple suivant :

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

Les notifications peuvent être de l'un des types de messages suivants.

Type de message	Description
ComplianceChangeNotification	Le type de conformité d'une ressource qui AWS Config évalue a changé. Le type de conformité indique si la ressource est conforme à une AWS Config règle spécifique, et il est représenté par la `ComplianceType` clé du message.

Type de message	Description
	Le message contient des objets `newEvaluationResult` et `oldEvaluationResult` de comparaison.
ConfigRulesEvaluationStarted	AWS Config a commencé à évaluer votre règle par rapport aux ressources spécifiées.
ConfigurationSnapshotDeliveryStarted	AWS Config a commencé à envoyer l'instantané de configuration à votre compartiment Amazon S3. Le nom du compartiment Amazon S3 est fourni pour la clé `s3Bucket` dans le message.
ConfigurationSnapshotDeliveryCompleted	AWS Config a livré avec succès l'instantané de configuration à votre compartiment Amazon S3.
ConfigurationSnapshotDeliveryFailed	AWS Config n'a pas réussi à fournir l'instantané de configuration à votre compartiment Amazon S3.
ConfigurationHistoryDeliveryCompleted	AWS Config a transmis avec succès l'historique de configuration à votre compartiment Amazon S3.
ConfigurationItemChangeNotification	Une ressource a été créée, supprimée ou modifiée dans la configuration. Ce message inclut les détails de l'élément de configuration AWS Config créé pour cette modification, ainsi que le type de modification. Ces notifications sont diffusées quelques minutes après un changement et sont communément appelées flux de configuration.

Type de message	Description
OversizedConfigurationItemChangeNotification	Ce type de message est envoyé lorsqu'un e notification de changement d'élément de configuration dépasse la taille maximale autorisée par Amazon SNS. Le message contient un récapitulatif de l'élément de configuration. À l'exception des messages SMS, les messages Amazon SNS peuvent contenir jusqu'à 256 Ko de données texte, y compris du XML, du JSON et du texte non formaté. Vous pouvez afficher la notification complète dans l'emplacement de compartiment Amazon S3 spécifié.
OversizedConfigurationItemChangeDeliveryFailed	AWS Config n'a pas réussi à envoyer la notification de modification d'un élément de configuration surdimensionné à votre compartiment Amazon S3.

Pour des exemples de notifications, consultez Notifications envoyées par AWS Config à une rubrique Amazon SNS. Pour plus d'informations sur Amazon SNS, consultez le Guide du développeur d'Amazon Simple Notification Service.

> **Note**
>
> Pourquoi ne puis-je pas voir mes dernières modifications de configuration ?
> AWS Config enregistre généralement les modifications de configuration de vos ressources juste après la détection d'une modification, ou à la fréquence que vous spécifiez. Cependant, cela se fait dans la mesure du possible et peut parfois prendre plus de temps. Si les problèmes persistent après un certain temps, contactez AWS Supportet fournissez vos AWS Config statistiques prises en charge par Amazon CloudWatch. Pour plus d'informations sur ces mesures, consultez la section Mesures AWS Config d'utilisation et de réussite.

Contrôlez l'accès à AWS Config

AWS Identity and Access Management est un service Web qui permet aux clients d'Amazon Web Services (AWS) de gérer les utilisateurs et les autorisations des utilisateurs.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Concepts

AWS Config fournit une vue détaillée des ressources qui vous sont associées Compte AWS, notamment de la manière dont elles sont configurées, de la manière dont elles sont liées les unes aux autres et de l'évolution des configurations et de leurs relations au fil du temps. Examinons de plus près les concepts de AWS Config.

Table des matières

- AWS Config Interfaces
  - AWS Config Console
  - AWS Config CLI
  - AWS Config API
  - AWS Config SDK
- Gestion des ressources

- AWS Ressources
- Relation de ressource
- Enregistreur de configuration
- Canal de livraison
  - Éléments de configuration
  - Historique des configurations
  - Instantané de configuration
  - Flux des configurations
- AWS Config Règles
  - AWS Config Règles gérées
  - AWS Config Règles personnalisées
  - Types de déclencheurs
  - Modes d'évaluation
- Packs de conformité
- Regroupement des données de plusieurs comptes et plusieurs régions
  - Compte source
  - Région source
  - Agrégateur
  - Compte Aggregator
  - Autorisation

AWS Config Interfaces

AWS Config Console

Vous pouvez gérer le service à l'aide de la AWS Config console. Pour plus d'informations sur le AWS Management Console, consultez AWS Management Console.

AWS Config CLI

AWS Command Line Interface Il s'agit d'un outil unifié avec lequel vous pouvez interagir AWS Config depuis la ligne de commande. Pour plus d'informations, consultez le Guide de l'utilisateur

AWS Command Line Interface. Pour une liste complète des commandes AWS Config CLI, voir Commandes disponibles.

AWS Config API

Outre la console et la CLI, vous pouvez également utiliser les API AWS Config RESTful pour programmer AWS Config directement. Pour plus d'informations, consultez la page Référence de l'API AWS Config.

AWS Config SDK

Au lieu d'utiliser l' AWS Config API, vous pouvez utiliser l'un des AWS SDK. Chaque Kit de développement logiciel (SDK) se compose de bibliothèques et d'exemples de code pour différents langages et plateformes de programmation. Ils facilitent la création par programmation d'un accès à AWS Config. Par exemple, vous pouvez utiliser des Kits de développement logiciel (SDK) pour signer de façon chiffrée des demandes, gérer les erreurs et lancer de nouvelles tentatives de demande automatiquement. Pour plus d'informations, consultez la page Outils pour Amazon Web Services.

Gestion des ressources

La compréhension des composants de base de vous AWS Config aidera à suivre l'inventaire et les modifications des ressources et à évaluer les configurations de vos AWS ressources.

AWS Ressources

AWS les ressources sont des entités que vous créez et gérez à l' AWS Management Console aide de la AWS Command Line Interface (CLI), AWS des SDK ou des outils AWS partenaires. Les exemples de AWS ressources incluent les instances Amazon EC2, les groupes de sécurité, les Amazon VPC et Amazon Elastic Block Store. AWS Config fait référence à chaque ressource à l'aide de son identifiant unique, tel que l'ID de ressource ou un Amazon Resource Name (ARN). Pour obtenir la liste des types de ressources AWS Config compatibles, consultezTypes de ressource pris en charge.

Relation de ressource

AWS Config découvre AWS les ressources de votre compte, puis crée une carte des relations entre les AWS ressources. Par exemple, une relation peut inclure un volume `vol-123ab45d` attaché à une instance Amazon EC2 `i-a1b2c3d4`, elle-même associée au groupe de sécurité `sg-ef678hk`.

Pour plus d'informations, consultez Types de ressource pris en charge.

Enregistreur de configuration

L'enregistreur de configuration stocke les configurations des ressources prises en charge dans votre compte en tant qu'éléments de configuration. Vous devez d'abord créer l'enregistreur de configuration, puis le démarrer avant de commencer l'enregistrement. Vous pouvez arrêter et redémarrer l'enregistreur de configuration à tout moment. Pour plus d'informations, consultez Gestion de l'enregistreur de configuration.

Par défaut, l'enregistreur de configuration enregistre toutes les ressources prises en charge dans la région où AWS Config il est exécuté. Vous pouvez créer un enregistreur de configuration personnalisé qui enregistre uniquement les types de ressource que vous indiquez. Pour plus d'informations, consultez AWS Ressources d'enregistrement.

Si vous utilisez la AWS Management Console ou la CLI pour activer le service, crée et démarre AWS Config automatiquement un enregistreur de configuration pour vous.

Canal de livraison

Comme il enregistre AWS Config en permanence les modifications apportées à vos AWS ressources, il envoie des notifications et des états de configuration mis à jour via le canal de livraison. Vous pouvez gérer le canal de diffusion pour contrôler l'endroit où les mises à jour de configuration sont AWS Config envoyées.

Éléments de configuration

Un élément de configuration représente une point-in-time vue des différents attributs d'une AWS ressource prise en charge qui existe dans votre compte. Les composants d'un élément de configuration incluent les métadonnées, les attributs, les relations, la configuration actuelle et les événements connexes. AWS Config crée un élément de configuration chaque fois qu'il détecte une modification d'un type de ressource qu'il enregistre. Par exemple, si vous AWS Config enregistrez des compartiments Amazon S3, AWS Config crée un élément de configuration chaque fois qu'un compartiment est créé, mis à jour ou supprimé. Vous pouvez également sélectionner de AWS Config créer un élément de configuration à la fréquence d'enregistrement que vous avez définie.

Pour plus d'informations, consultez Components of a Configuration Item et Sélection des ressources qui sont enregistrées | Fréquence d'enregistrement.

Historique des configurations

Un historique de configuration est un ensemble d'éléments de configuration pour une ressource donnée sur une période donnée. Il permet de répondre aux questions concernant, par exemple, la date de création de la ressource, la configuration de la ressource au cours du dernier mois, ainsi que les changements de configuration effectués hier à 9h. L'historique de configuration est disponible dans plusieurs formats. AWS Config fournit automatiquement un fichier d'historique de configuration pour chaque type de ressource enregistré dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez sélectionner une ressource donnée dans la AWS Config console et accéder à tous les éléments de configuration précédents pour cette ressource à l'aide de la chronologie. En outre, vous pouvez accéder aux éléments de l'historique de configuration pour une ressource à partir de l'interface API.

Pour plus d'informations, consultez les sections Affichage AWS des configurations et de l'historique des AWS ressources et Gestion des configurations et de l'historique des ressources.

Instantané de configuration

Un instantané de configuration est un ensemble d'éléments de configuration pour les ressources prises en charge de votre compte. Cet instantané de la configuration est une image complète des ressources qui sont en cours d'enregistrement et de leur configuration. Il peut être un outil utile pour la validation de votre configuration. Par exemple, vous pouvez examiner l'instantané de configuration régulièrement pour les ressources qui sont configurées de façon incorrecte ou qui ne devraient pas exister. Il est disponible dans plusieurs formats. Vous pouvez faire en sorte que l'instantané de configuration soit diffusé vers un compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez. En outre, vous pouvez sélectionner un moment dans la AWS Config console et parcourir l'instantané des éléments de configuration à l'aide des relations entre les ressources.

Flux des configurations

Un flux de configuration est une liste automatiquement mise à jour de tous les éléments de configuration pour les ressources en cours AWS Config d'enregistrement. Chaque fois qu'une ressource est créée, modifiée ou supprimée, AWS Config crée un élément de configuration et l'ajoute dans le flux de configuration. Le flux de configuration fonctionne en utilisant la rubrique Amazon Simple Notification Service (Amazon SNS) de votre choix. Le flux de configuration est utile pour observer les modifications de configuration au fur et à mesure qu'elles se produisent afin de détecter les problèmes potentiels, de générer des notifications si certaines ressources sont modifiées ou de mettre à jour les systèmes externes qui doivent refléter la configuration de vos AWS ressources.

AWS Config Règles

Une AWS Config règle représente les paramètres de configuration souhaités pour des AWS ressources spécifiques ou pour une ressource complète Compte AWS. Si une ressource ne passe pas la vérification des règles, AWS Config signale la ressource et la règle comme non conformes et vous en AWS Config informe via Amazon SNS. Les résultats d'évaluation possibles pour une AWS Config règle sont les suivants :

- `COMPLIANT` - la règle satisfait aux conditions du contrôle de conformité.
- `NON_COMPLIANT` - la règle ne satisfait pas aux conditions du contrôle de conformité.
- `ERROR` - l'un des paramètres obligatoires/facultatifs n'est pas valide, n'est pas du bon type ou est mal formaté.
- `NOT_APPLICABLE` - utilisé pour filtrer les ressources auxquelles la logique de la règle ne peut s'appliquer. Par exemple, la règle alb-desync-mode-check ne vérifie que les Application Load Balancers et ignore les Network Load Balancers et les équilibreurs de charge de passerelle.

Il existe deux types de règles : les règles AWS Config gérées et les règles AWS Config personnalisées. Pour plus d'informations sur la structure des définitions de règles et des métadonnées des règles, voir Composants d'une AWS Config règle.

AWS Config Règles gérées

AWS Config Les règles gérées sont des règles prédéfinies et personnalisables créées par AWS Config. Pour obtenir la liste des règles gérées, consultez la section Liste des règles AWS Config gérées.

AWS Config Règles personnalisées

AWS Config Les règles personnalisées sont des règles que vous créez de toutes pièces. Il existe deux manières de créer des règles AWS Config personnalisées : avec les fonctions Lambda (Guide du AWS Lambda développeur) et avec Guard (Guard GitHub Repository), un policy-as-code langage. AWS Config les règles personnalisées créées avec AWS Lambda sont appelées règles Lambda AWS Config personnalisées et les règles AWS Config personnalisées créées avec Guard sont appelées règles de politique AWS Config personnalisées.

Pour une présentation expliquant comment créer des règles de stratégie AWS Config personnalisées, voir Création de règles de stratégie AWS Config personnalisées. Pour une présentation expliquant

comment créer des règles Lambda AWS Config personnalisées, voir Création de règles Lambda AWS Config personnalisées.

Types de déclencheurs

Après avoir ajouté une règle à votre compte, AWS Config comparez vos ressources aux conditions de cette règle. Après cette évaluation initiale, AWS Config continue à exécuter des évaluations chaque fois qu'une évaluation est déclenchée. Les déclencheurs d'évaluation sont définis dans le cadre de la règle et peuvent inclure les types suivants.

Type de déclencheur	Description
Configuration changes	AWS Config exécute des évaluations pour la règle lorsqu'une ressource correspond au champ d'application de la règle et qu'il y a un changement de configuration de la ressource. L'évaluation s'exécute après l' AWS Config envoi d'une notification de modification d'élément de configuration. Vous choisissez quelles ressources déclenche nt l'évaluation en définissant la portée de la règle. La portée peut inclure les éléments suivants : • Un ou plusieurs types de ressources • Une combinaison d'un type de ressource et d'un ID de ressource • Une combinaison d'une clé de balise et d'une valeur • Lorsqu'une ressource enregistrée est créée, mise à jour ou supprimée AWS Config exécute l'évaluation lorsqu'il détecte une modification apportée à une ressource correspondant au champ d'applica tion de la règle. Vous pouvez utiliser la portée

Type de déclencheur	Description
	afin de définir les ressources qui déclenchent des évaluations.
Périodique	AWS Config exécute des évaluations de la règle à la fréquence que vous choisissez, par exemple toutes les 24 heures.
Hybride	Certaines règles comportent à la fois des changements de configuration et des déclencheurs périodiques. Pour ces règles, AWS Config évalue vos ressources lorsqu'il détecte un changement de configuration et également à la fréquence que vous spécifiez.

Modes d'évaluation

Il existe deux modes d'évaluation des AWS Config règles.

Mode d'évaluation	Description
Proactif	Utilisez l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriété s de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région. Pour plus d'informations, consultez Modes d'évaluation. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.

Mode d'évaluation	Description
Détective	Utilisez l'évaluation détective pour évaluer les ressources déjà déployées. Ce type d'évaluat ion vous permet d'évaluer les paramètres de configuration de vos ressources existantes.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Packs de conformité

Un pack de conformité est un ensemble de AWS Config règles et d'actions correctives qui peuvent être facilement déployées en tant qu'entité unique dans un compte et une région ou au sein d'une organisation dans. AWS Organizations

Les packs de conformité sont créés au moyen d'un modèle YAML qui contient la liste des règles gérées ou personnalisées et des actions de correction AWS Config . Vous pouvez déployer le modèle à l'aide de la console AWS Config ou de la AWS CLI.

Pour démarrer rapidement et évaluer votre AWS environnement, utilisez l'un des exemples de modèles de pack de conformité. Vous pouvez également créer un fichier YAML de pack de conformité à partir de zéro sur la base du pack de conformité personnalisé. Un pack de conformité personnalisé est un ensemble unique de AWS Config règles et d'actions correctives que vous pouvez déployer ensemble dans un compte et une AWS région, ou au sein d'une organisation dans. AWS Organizations

Les contrôles de processus sont un type de AWS Config règle qui vous permet de suivre vos tâches externes et internes qui nécessitent une vérification dans le cadre des packs de conformité. Ces vérifications peuvent être ajoutées à un pack de conformité existant ou à un nouveau pack de conformité. Vous pouvez suivre l'ensemble de la conformité, y compris AWS Config les durées et les contrôles manuels, en un seul endroit.

Regroupement des données de plusieurs comptes et plusieurs régions

L'agrégation de données multicomptes et multirégions vous AWS Config permet d'agréger les données de AWS Config configuration et de conformité de plusieurs comptes et régions dans un seul compte. L'agrégation de données multicomptes et multirégions est utile aux administrateurs informatiques centraux afin de contrôler la conformité de plusieurs Comptes AWS entreprises. L'utilisation d'agrégateurs n'entraîne aucun coût supplémentaire.

Compte source

Un compte source est le compte Compte AWS à partir duquel vous souhaitez agréger les données de configuration et de conformité des AWS Config ressources. Un compte source peut être un compte individuel ou une organisation dans AWS Organizations. Vous pouvez fournir des comptes sources individuellement ou vous pouvez les récupérer via AWS Organizations.

Région source

Une région source est la AWS région à partir de laquelle vous souhaitez agréger les données AWS Config de configuration et de conformité.

Agrégateur

Un agrégateur collecte des données AWS Config de configuration et de conformité à partir de plusieurs comptes sources et régions. Créez un agrégateur dans la région où vous souhaitez consulter les données de AWS Config configuration et de conformité agrégées.

> **Note**
>
> Les agrégateurs fournissent une vue en lecture seule des comptes source et des régions que l'agrégateur est autorisé à consulter en répliquant les données des comptes sources vers le compte agrégateur. Les agrégateurs ne fournissent pas d'accès mutant à un compte ou à une région source. Par exemple, cela signifie que vous ne pouvez pas déployer de règles via un agrégateur ou transférer des fichiers instantanés vers un compte ou une région source via un agrégateur.

Compte Aggregator

Un compte Aggregator est un compte dans lequel vous créez un agrégateur.

Autorisation

En tant que propriétaire du compte source, l'autorisation fait référence aux autorisations que vous accordez à un compte agrégateur et à une région pour collecter vos données de AWS Config configuration et de conformité. Aucune autorisation n'est requise si vous regroupez des comptes source qui font partie de AWS Organizations.

Prise en charge de la région

> **Note**
>
> Certaines fonctionnalités de ne AWS Config sont prises en charge que dans un sous-ensemble des AWS régions où elles AWS Config sont prises en charge.
>
> Gestion des ressources
>
> - Pour obtenir la liste des types de AWS ressources pris en charge dans quelles régions, consultez la section Couverture des ressources par disponibilité des régions.
>
> AWS Config Règles
>
> - Pour obtenir la liste des AWS Config règles prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.
> - Pour obtenir la liste des régions qui prennent en charge le déploiement organisationnel des AWS Config règles, voir Règles organisationnelles | Support régional.
> - Pour obtenir la liste des régions qui prennent en charge les mesures correctives relatives AWS Config aux règles, voir Actions correctives | Support régional.
>
> Packs de conformité
>
> - Pour obtenir la liste des régions qui prennent en charge les packs de conformité et le déploiement organisationnel des packs de conformité, consultez Packs de conformité | Prise en charge des régions.
>
> Agrégateurs
>
> - Pour obtenir la liste des régions qui prennent en charge les agrégateurs, consultez Agrégateurs | Prise en charge des régions.

Requêtes avancées

- Pour obtenir la liste des régions qui prennent en charge les requêtes avancées, consultez Requêtes avancées | Prise en charge des régions.
- Pour connaître la liste des régions qui prennent en charge le processeur de requêtes en langage naturel pour les requêtes avancées, voir Processeur de requêtes en langage naturel pour les requêtes avancées | Prise en charge régionale.

Le tableau suivant répertorie les AWS régions dans lesquelles vous pouvez activer AWS Config.

Nom de la région	Région	Point de terminaison	Protocole
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
Afrique (Le Cap)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asie-Pacifique	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
(Hong Kong)			
Asie-Pacifique (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada Ouest (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Espagne)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israël (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Moyen-Orient (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Service Limits

Le tableau suivant décrit les limites au sein d'AWS Config. Sauf indication contraire, les quotas peuvent être augmentés sur simple demande. Vous pouvez demander une augmentation de quota.

Pour plus d'informations sur les autres limites dans AWS, consultez Limites de service AWS.

Limites du service AWS Config

Description	Valeur limite	Peut être augmenté
Nombre maximal de règles AWS Config par région et par compte	1 000	Non
Nombre maximal de balises par ressource	50	Non

Packs de conformité pour un compte unique

Description	Valeur limite	Peut être augmenté
Nombre maximal de packs de conformité par compte	50	Non
Nombre maximal de règles AWS Config par pack de conformité	130	Non

> **Note**
>
> Les règles AWS Config contenues dans les packs de conformité sont prises en compte dans la limite du nombre maximal de règles AWS Config par région et par compte.

Packs de conformité pour une organisation

Description	Valeur limite	Peut être augmenté
Nombre maximal de packs de conformité par organisation	50	Non
Nombre maximal de règles AWS Config par pack de conformité pour une organisation	130	Non

> **Note**
>
> Le déploiement au niveau de l'organisation est pris en compte dans la limite appliquée aux comptes enfants. Les règles AWS Config contenues dans les packs de conformité sont prises en compte dans la limite du nombre maximal de règles AWS Config par région et par compte.

Agrégateurs

Description	Valeur limite	Peut être augmenté
Nombre maximal d’agrégateurs de configuration	50	Oui
Nombre maximal de comptes dans un agrégateur	10 000	Non
Nombre maximal de comptes ajoutés ou supprimés par semaine pour tous les agrégateurs	1 000	Oui

Requêtes avancées

Description	Valeur limite	Peut être augmenté
Nombre maximal de requêtes enregistrées dans un seul compte et une seule région	300	Oui

AWS Intégrations de services avec AWS Config

AWS Config prend en charge les intégrations avec plusieurs autres AWS services.

AWS Organizations

Vous pouvez l'utiliser AWS Organizations pour définir les comptes à utiliser pour la fonctionnalité d'agrégation AWS Config de données multicomptes et multirégions de la société. AWS Organizations est un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée. En fournissant vos AWS Organizations coordonnées, vous pouvez surveiller l'état de conformité au sein de votre organisation. Pour plus d'informations, AWS Config et AWS Organizations dans le guide de AWS Organizations l'utilisateur.

AWS Control Tower

AWS Control Tower s'active AWS Config sur tous les comptes inscrits, afin qu'il puisse surveiller la conformité grâce à des contrôles de détection, enregistrer les modifications des ressources et fournir des journaux des modifications des ressources au compte d'archivage des journaux. Pour plus d'informations, consultez la section Surveiller les modifications des ressources AWS Config dans le Guide de AWS Control Tower l'utilisateur.

AWS CloudTrail

AWS Config s'intègre AWS CloudTrail pour corréler les modifications de configuration à des événements particuliers de votre compte. Vous pouvez utiliser les CloudTrail journaux pour obtenir les détails de l'événement à l'origine de la modification, notamment l'auteur de la demande, l'heure et l'adresse IP à partir de laquelle vous l'avez demandée. Vous pouvez accéder à la AWS Config chronologie depuis la CloudTrail console pour consulter les modifications de configuration liées à vos activités AWS d'API.

Pour plus d'informations, consultez les sections Journalisation des appels d' AWS Config API AWS CloudTrail dans le guide du AWS Config développeur et Création d'un magasin de données d'événements pour les éléments de AWS Config configuration avec la console dans le guide de AWS CloudTrail l'utilisateur.

AWS Security Hub

AWS Security Hub centralise les contrôles de sécurité provenant d'autres AWS services, y compris AWS Config les règles. Security Hub active et contrôle AWS Config les règles pour vérifier que les configurations de vos ressources sont conformes aux meilleures pratiques. Activez AWS Config cette option sur tous les comptes dans toutes les régions où Security Hub est installé pour effectuer des contrôles de sécurité sur les ressources de votre environnement. Pour plus d'informations, consultez la section AWS Services qui envoient des résultats à Security Hub dans le Guide de AWS Security Hub l'utilisateur.

AWS Audit Manager

Vous pouvez utiliser Audit Manager pour saisir les AWS Config évaluations comme preuves pour les audits. Lorsque vous créez ou modifiez un contrôle personnalisé, vous pouvez spécifier une ou plusieurs AWS Config règles en tant que mappage des sources de données pour la collecte de preuves. AWS Config effectue des contrôles de conformité sur la base de ces règles, et Audit Manager rapporte les résultats à titre de preuve du contrôle de conformité. Pour plus d'informations, consultez la section AWS Config Règles prises en charge AWS Audit Manager dans le Guide de AWS Audit Manager l'utilisateur.

AWS Systems Manager

AWS Config s'intègre à Systems Manager pour enregistrer les modifications de configuration des logiciels sur vos instances et serveurs Amazon EC2 dans votre environnement sur site. Grâce à cette intégration, vous pouvez gagner en visibilité sur les configurations du système d'exploitation (OS), les mises à jour au niveau du système, les applications installées, la configuration réseau, etc. AWS Config fournit également un historique des modifications de configuration au niveau du système d'exploitation et du système, ainsi que des modifications de configuration d'infrastructure enregistrées pour les instances Amazon EC2. Vous pouvez accéder à la AWS Config chronologie depuis la console Systems Manager pour consulter les modifications de configuration de vos instances Amazon EC2 gérées. Vous pouvez l'utiliser AWS Config pour consulter l'historique d'inventaire de Systems Manager et suivre les modifications apportées à toutes vos instances gérées.

Pour plus d'informations, voir Intégration aux AWS services | Gestion et gouvernance, enregistreur AWS Config de configuration et déploiement du pack de AWS Config conformité dans le guide de l'AWS Systems Manager utilisateur.

AWS Firewall Manager

Pour utiliser Firewall Manager, vous devez l'activer AWS Config pour chacun de vos comptes AWS Organizations membres. Lorsque de nouvelles applications sont créées, Firewall Manager est le seul service permettant de créer des règles de pare-feu, de créer des politiques de sécurité et de les appliquer de manière cohérente. Pour plus d'informations, consultez la section Activer AWS Config dans AWS WAF le AWS Firewall Manager et le Guide AWS Shield Advanced du développeur.

> **Note**
>
> Firewall Manager s'appuie sur l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu. Pour plus d'informations sur l'enregistrement en continu et l'enregistrement quotidien, consultez la section Fréquence d'enregistrement.

Hôtes dédiés Amazon EC2

AWS Config s'intègre aux hôtes dédiés Amazon EC2 pour évaluer la conformité des licences. AWS Config enregistre le lancement, l'arrêt ou l'arrêt des instances sur un hôte dédié, et associe ces informations aux informations au niveau de l'hôte et de l'instance relatives aux licences logicielles, telles que l'identifiant de l'hôte, les identifiants Amazon Machine Image (AMI), le nombre de sockets et les cœurs physiques. Cela vous permet de l'utiliser AWS Config comme source de données pour vos rapports sur les licences. Vous pouvez accéder à la AWS Config chronologie depuis la console Amazon EC2 Dedicated Hosts pour consulter les modifications de configuration de vos hôtes dédiés Amazon EC2.

Pour plus d'informations, consultez la section Suivi des modifications de configuration dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Linux ou Suivi des modifications de configuration dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Windows.

Application Load Balancers

AWS Config s'intègre au service Elastic Load Balancing (ELB) pour enregistrer les modifications de configuration apportées aux équilibreurs de charge des applications. AWS Config inclut également les relations avec les groupes de sécurité, les VPC et les sous-réseaux Amazon EC2 associés. Vous pouvez utiliser ces informations à des fins d'analyse de sécurité et de résolution des problèmes. Par exemple, vous pouvez vérifier quels groupes de sécurité sont associés à votre Application Load Balancer à tout moment. Vous pouvez accéder à la AWS Config chronologie depuis la console ELB pour consulter les modifications de configuration de vos équilibreurs de charge d'application.

AWS CodeBuild

AWS Config fournit un inventaire de vos AWS ressources et un historique des modifications de configuration apportées à ces ressources. AWS Config supports AWS CodeBuild ; en tant que AWS ressource, ce qui signifie que le service peut suivre vos CodeBuild projets. Pour plus d'informations, consultez la section Utiliser AWS Config avec CodeBuild un échantillon dans le guide de AWS CodeBuild l'utilisateur.

AWS X-Ray

AWS X-Ray s'intègre AWS Config pour enregistrer les modifications de configuration apportées à vos ressources de chiffrement X-Ray. Vous pouvez l'utiliser AWS Config pour inventorier les ressources de chiffrement de X-Ray, vérifier l'historique de configuration de X-Ray et envoyer des notifications en fonction des modifications apportées aux ressources. Pour plus d'informations, consultez la section Suivi des modifications de configuration du chiffrement de X-Ray AWS Config dans le manuel du AWS X-Ray développeur.

Connecteur AWS Service Management

Le formulaire Connecteur AWS Service Management ServiceNow peut synchroniser les AWS Config données de plusieurs comptes et régions à l'aide d'un agrégateur. Pour plus d'informations, consultez la section Intégration AWS Config ServiceNow dans le guide de Connecteur AWS Service Management l'administrateur.

Amazon API Gateway

Vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à vos ressources API API Gateway et envoyer des notifications en fonction des modifications apportées aux ressources. Il peut être utile de conserver un historique des modifications de configuration

apportées aux ressources API Gateway pour un dépannage et un audit opérationnel ainsi que pour des cas d'utilisation de conformité. Pour plus d'informations, consultez la section Surveillance de la configuration de l'API API Gateway AWS Config dans le guide du développeur d'API Gateway.

Informations supplémentaires et ressources connexes

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

- AWS Config— La page Web principale contenant des informations sur AWS Config.
- Tarification AWS Config
- FAQ technique
- AWS Config Kit de développement de règles (RDK) : outil open source qui vous aide à configurer AWS Config, à créer des règles, puis à les tester à l'aide de différents types de AWS ressources.
- Partenaires : liens vers des produits partenaires entièrement intégrés pour vous aider AWS Config à visualiser, surveiller et gérer les données issues de votre flux de configuration, de vos instantanés de configuration ou de votre historique de configuration.

- Cours et ateliers — Liens vers des cours spécialisés et basés sur des rôles, ainsi que des ateliers à votre rythme pour vous aider à perfectionner vos AWS compétences et à acquérir une expérience pratique.
- AWS Centre pour développeurs : découvrez les didacticiels, téléchargez des outils et découvrez les événements AWS destinés aux développeurs.
- AWS Outils de développement : liens vers des outils de développement, des SDK, des boîtes à outils IDE et des outils de ligne de commande pour le développement et la gestion AWS d'applications.
- Centre de ressources pour la mise en route : découvrez comment configurer votre application Compte AWS, rejoindre la AWS communauté et lancer votre première application.
- Tutoriels pratiques — Suivez les step-by-step didacticiels pour lancer votre première application sur AWS.
- AWS Livres blancs : liens vers une liste complète de livres AWS blancs techniques, traitant de sujets tels que l'architecture, la sécurité et l'économie, rédigés par des architectes de AWS solutions ou d'autres experts techniques.
- AWS Support Centre — Le centre de création et de gestion de vos AWS Support dossiers. Comprend également des liens vers d'autres ressources utiles, telles que des forums, des FAQ techniques, l'état de santé du service et AWS Trusted Advisor.

- AWS Support— La principale page Web contenant des informations sur AWS Support un one-on-one canal d'assistance à réponse rapide pour vous aider à créer et à exécuter des applications dans le cloud.
- Contactez-nous : point de contact central pour toute question relative à la facturation AWS , à votre compte, aux événements, à des abus ou à d'autres problèmes.
- AWS Conditions du site — Informations détaillées sur nos droits d'auteur et notre marque commerciale ; votre compte, votre licence et l'accès au site ; et d'autres sujets.

AWS Kits de développement logiciel pour AWS Config

Un kit de développement AWS logiciel (SDK) facilite la création d'applications qui accèdent à des services d' AWS infrastructure rentables, évolutifs et fiables. Avec les kits de développement logiciel AWS vous pouvez démarrer en quelques minutes avec un package unique, téléchargeable qui inclut la bibliothèque, des exemples de code et de la documentation de référence. Le tableau suivant répertorie les SDK et les bibliothèques tierces disponibles auxquels vous pouvez accéder AWS Config par programmation.

Type d'accès	Description
AWS SDK	AWS fournit les SDK suivants : • AWS Documentation du SDK pour C++ • AWS Mobile SDK for iOS Documentation • Documentation sur le kit SDK AWS pour Go • AWS SDK for Java Documentation • AWS SDK pour la documentation JavaScript • AWS SDK for .NET Documentation • AWS SDK for PHP Documentation • AWS SDK for Python (Boto) Documentation • AWS SDK for Ruby Documentation
Bibliothèques tierces	Les développeurs de la communauté des AWS développeurs fournissent également leurs propres bibliothèques, que vous pouvez trouver dans les centres de AWS développement suivants :

Type d'accès	Description
	• AWS Centre pour développeurs Java • Centre pour développeurs AWS JavaScript • AWS Centre pour développeurs PHP • AWS Centre pour développeurs Python • AWS Centre de développement Ruby • AWS Centre pour développeurs Windows et .NET

Commencer avec AWS Config

AWS Config fournit une vue détaillée de la configuration des AWS ressources de votre Compte AWS. Vous pouvez ainsi examiner les modifications apportées aux configurations et aux relations entre les AWS ressources, explorer l'historique de configuration des ressources et utiliser des règles pour déterminer la conformité. AWS Config Pour plus d'informations, voir Qu'est-ce que c'est AWS Config ? et comment AWS Config fonctionne.

S'inscrire à AWS

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d‘inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l‘utilisateur racine a accès à l‘ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l‘activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Façons de démarrer avec AWS Config

Après vous être inscrit à un Compte AWS, vous pouvez AWS Config commencer à utiliser la AWS Management Console AWS CLI ou les AWS SDK.

- Configuration à l' AWS Config aide de la console
- Configuration AWS Config avec le AWS CLI
- Utilisation AWS Config du service avec le AWS SDK

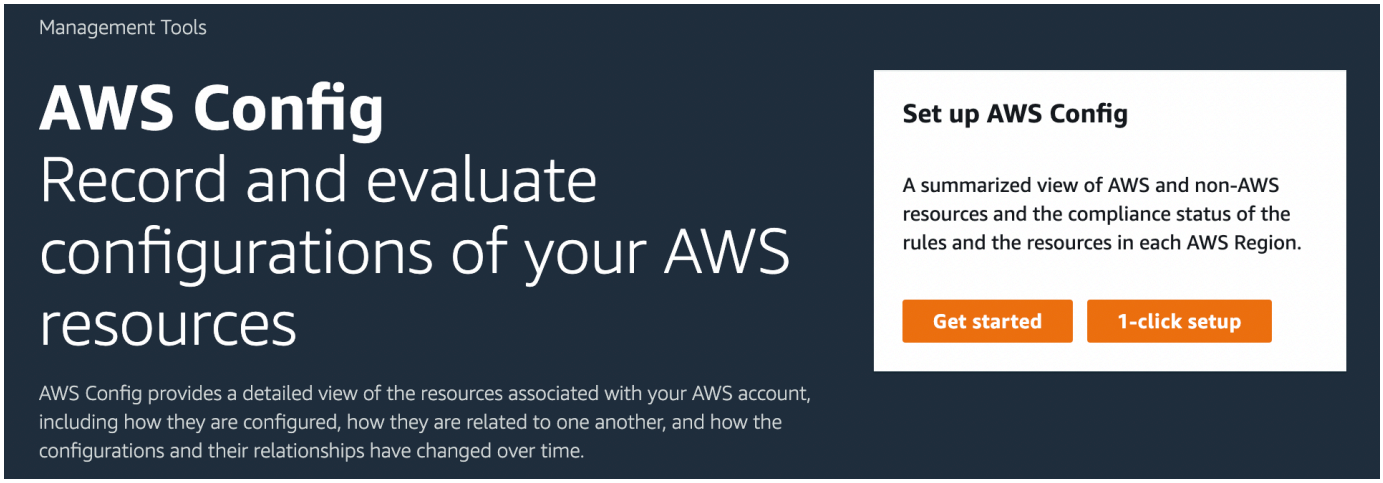
Configuration à l' AWS Config aide de la console

AWS Management Console Il fournit un processus de configuration rapide et rationalisé AWS Config.

Configuration

Pour configurer à l' AWS Config aide de la console

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Si c'est la première fois que vous ouvrez la AWS Config console ou que vous la configurez AWS Config dans une nouvelle région, la page de la AWS Config console se présente comme suit :



3. Choisissez la configuration en un clic pour lancer AWS Config conformément aux AWS meilleures pratiques. Vous pouvez également sélectionner Mise en route pour bénéficier d'un processus de configuration plus détaillé.

Rubriques

- Configuration en un clic
- Configuration manuelle

Configuration en un clic

AWS Config La configuration en un clic permet de simplifier le processus de démarrage pour les clients de la AWS Config console en réduisant le nombre de sélections manuelles. Pour passer en revue toutes les sélections manuelles du processus de configuration, voir Configuration manuelle.

Pour configurer à l'aide de la console AWS Config à l'aide de la configuration en un clic

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Sélectionnez la configuration en un clic.

La page de configuration comprend trois étapes. Toutefois, vous êtes automatiquement dirigé vers l'étape 3 (vérification) grâce au flux de travail de la configuration en un clic. Vous trouverez ci-dessous une description détaillée de cette procédure.

- Paramètres : pour sélectionner la manière dont la AWS Config console enregistre les ressources et les rôles, et pour choisir où l'historique de configuration et les fichiers instantanés de configuration sont envoyés.
- Règles : pour les régions qui prennent en charge les règles, cette sous-section vous permet de configurer les règles AWS gérées initiales que vous pouvez ajouter à votre compte.

  Après la configuration, AWS Config évaluera vos AWS ressources par rapport aux règles que vous avez choisies. Des règles supplémentaires peuvent être créées et les règles existantes peuvent être mises à jour dans votre compte après la configuration. Pour plus d'informations sur les règles, consultez la section Gestion de vos AWS Config règles.
- Révision : pour vérifier les détails de votre configuration.

Paramètres

Stratégie d'enregistrement

L'option permettant d'enregistrer tous les types de ressources avec des remplacements personnalisables est sélectionnée pour vous. AWS Config enregistrera tous les types de ressources pris en charge actuels et futurs dans cette région. Pour plus d'informations, consultez Types de ressources pris en charge.

- Paramètres par défaut

  La fréquence d'enregistrement par défaut est définie sur Continu pour vous. Cela signifie qu'il AWS Config enregistre les modifications de configuration en continu chaque fois qu'une modification se produit.

  AWS Config prend également en charge la possibilité de régler la fréquence d'enregistrement sur Quotidien. Si vous sélectionnez cette option après la configuration, vous recevrez un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il diffère de l'élément de configuration enregistré précédemment. Pour plus d'informations, consultez Fréquence d'enregistrement.

> **Note**
>
> AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

- Paramètres de remplacement (facultatif)

  Après la configuration, vous pouvez éventuellement modifier la fréquence d'enregistrement de types de ressources spécifiques ou exclure certains types de ressources de l'enregistrement. Pour remplacer les paramètres par défaut, choisissez Paramètres dans le menu de navigation de gauche de la AWS Config console, puis sélectionnez Modifier.

Considérations relatives à l'enregistrement des ressources

Nombre élevé d' AWS Config évaluations

Vous remarquerez peut-être une augmentation de l'activité de votre compte lors de votre premier mois d'enregistrement avec AWS Config par rapport aux mois suivants. Au cours du processus de démarrage initial, AWS Config exécute des évaluations sur toutes les ressources de votre compte que vous avez sélectionnées AWS Config pour enregistrement.

Si vous exécutez des charges de travail éphémères, il se peut que vous constatiez une activité accrue d' AWS Config en raison de l'enregistrement des changements de configuration associés à la création et à la suppression de ces ressources temporaires. Une charge de travail éphémère est une utilisation temporaire des ressources informatiques chargées et exécutées si nécessaire. Il peut par exemple s'agir des instances Spot Amazon Elastic Compute Cloud (Amazon EC2), des tâches Amazon EMR et d' AWS Auto Scaling. Si vous souhaitez éviter l'augmentation de l'activité liée à l'exécution de charges de travail éphémères, vous pouvez configurer l'enregistreur de configuration pour exclure l'enregistrement de ces types de ressources, ou exécuter ces types de charges de travail dans un compte distinct en désactivant pour éviter d' AWS Config augmenter l'enregistrement des configurations et l'évaluation des règles.

Types de ressources mondiales | Les clusters Aurora mondiaux sont initialement inclus dans l'enregistrement

Le type de `AWS::RDS::GlobalCluster` ressource sera enregistré dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé.

Si vous ne souhaitez pas enregistrer `AWS::RDS::GlobalCluster` dans toutes les régions activées, vous pouvez exclure ce type de ressource de l'enregistrement après la configuration. Dans la barre de navigation de gauche, sélectionnez Paramètres, puis Modifier. Dans Modifier, accédez à Paramètres de remplacement dans la section Méthode d'enregistrement`AWS::RDS::GlobalCluster`, puis choisissez l'option « Exclure de l'enregistrement ».

Types de ressources mondiales | Les types de ressources IAM sont initialement exclus de l'enregistrement

« Tous les types de ressources IAM enregistrés au niveau mondial » sont initialement exclus de l'enregistrement pour vous aider à réduire vos coûts. Cela inclut les utilisateurs, les groupes et les rôles IAM, ainsi que les politiques gérées par le client. Choisissez Supprimer pour supprimer l'exclusion et inclure ces ressources dans votre enregistrement.

L'exception à cette note concerne la région USA Est (Virginie du Nord). Les types de ressources IAM enregistrés au niveau mondial sont initialement inclus dans la région USA Est (Virginie du Nord), car cette région fonctionne comme la région d'origine des types de ressources IAM mondiales.

En outre, les types de ressources IAM globaux (`AWS::IAM::User`, `AWS::IAM::Group``AWS::IAM::Role`, et`AWS::IAM::Policy`) ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Gouvernance des données

La période de conservation des données par défaut pour conserver les AWS Config données pendant 7 ans (2557 jours) est sélectionnée pour vous dans cette section.

L'option Utiliser un rôle AWS Config lié à un service existant est sélectionnée pour vous et définie sur le AWS Config rôle. Les rôles liés à un service sont prédéfinis par AWS Config et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services.

Mode de remise

L'option Choisir un compartiment dans votre compte est sélectionnée pour vous dans cette section. Cette sélection portera par défaut sur le compartiment de votre compte nommé dans le format`config-bucket-`*`accountid`*. Par exemple, `config-bucket-012345678901`. Si aucun compartiment n'a été créé dans ce format, il en sera créé un pour vous. Si vous souhaitez créer votre propre compartiment, consultez Créer un compartiment dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour plus d'informations sur les compartiments S3, consultez Présentation des compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

Règles

Sous Règles AWS gérées, aucune règle n'est sélectionnée pour vous à cette étape. Nous vous encourageons plutôt à créer et à mettre à jour des règles une fois que vous aurez terminé la configuration de votre compte.

Vérification

Vérifiez les détails AWS Config de votre configuration. Vous pouvez revenir en arrière pour modifier les changements apportés à chaque section. Choisissez Confirmer pour terminer la configuration AWS Config.

Configuration manuelle

Avec le flux de travail Get started, vous pouvez effectuer toutes les sélections manuelles du processus de configuration pour commencer à utiliser la AWS Config console. Pour un processus de démarrage simplifié, voir Configuration en un clic.

Pour effectuer la configuration à l' AWS Config aide de la console à l'aide de la commande Get started

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Sélectionnez Mise en route.

La page de configuration comprend trois étapes. Vous trouverez ci-dessous une description détaillée de cette procédure une fois que vous aurez choisi Mise en route.

- Paramètres : pour sélectionner la manière dont la AWS Config console enregistre les ressources et les rôles, et pour choisir où l'historique de configuration et les fichiers instantanés de configuration sont envoyés.
- Règles : pour les régions qui prennent en charge les règles, cette sous-section vous permet de configurer les règles AWS gérées initiales que vous pouvez ajouter à votre compte.

  Après la configuration, AWS Config évaluera vos AWS ressources par rapport aux règles que vous avez choisies. Des règles supplémentaires peuvent être créées et les règles existantes peuvent être mises à jour dans votre compte après la configuration. Pour plus d'informations sur les règles, consultez la section Gestion de vos AWS Config règles.

- Révision : pour vérifier les détails de votre configuration.

Paramètres

Stratégie d'enregistrement

Dans la section Méthode d'enregistrement, choisissez une stratégie d'enregistrement. Vous pouvez spécifier les AWS ressources que vous AWS Config souhaitez enregistrer.

All resource types with customizable overrides

Configuré AWS Config pour enregistrer les modifications de configuration pour tous les types de ressources pris en charge actuels et futurs dans cette région. Vous pouvez modifier la fréquence d'enregistrement de types de ressources spécifiques ou exclure certains types de ressources de l'enregistrement. Pour plus d'informations, consultez Types de ressources pris en charge.

- Paramètres par défaut

  Configurez la fréquence d'enregistrement par défaut de tous les types de ressources actuels et futurs pris en charge. Pour plus d'informations, consultez Fréquence d'enregistrement.

  - Enregistrement continu : AWS Config enregistre les modifications de configuration en continu chaque fois qu'une modification se produit.
  - Enregistrement quotidien : vous recevrez un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il est différent de l'élément de configuration enregistré précédemment.

  > **Note**
  >
  > AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

- Paramètres de remplacement

  Modifiez la fréquence d'enregistrement de types de ressources spécifiques ou excluez des types de ressources spécifiques de l'enregistrement. Si vous modifiez la fréquence d'enregistrement d'un type de ressource ou si vous arrêtez l'enregistrement d'un type de ressource, les éléments de configuration déjà enregistrés resteront inchangés.

Specific resource types

Défini AWS Config pour enregistrer les modifications de configuration uniquement pour les types de ressources que vous spécifiez.

- Types de ressources spécifiques

  Choisissez un type de ressource à enregistrer et sa fréquence. Pour plus d'informations, consultez Fréquence d'enregistrement.

  - Enregistrement continu : AWS Config enregistre les modifications de configuration en continu chaque fois qu'une modification se produit.
  - Enregistrement quotidien : vous recevrez un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il est différent de l'élément de configuration enregistré précédemment.

  > **Note**
  >
  > AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

  Si vous modifiez la fréquence d'enregistrement d'un type de ressource ou si vous arrêtez l'enregistrement d'un type de ressource, les éléments de configuration déjà enregistrés resteront inchangés.

Considérations relatives à l'enregistrement des ressources

Nombre élevé d' AWS Config évaluations

Vous remarquerez peut-être une augmentation de l'activité de votre compte lors de votre premier mois d'enregistrement avec AWS Config par rapport aux mois suivants. Au cours du processus de démarrage initial, AWS Config exécute des évaluations sur toutes les ressources de votre compte que vous avez sélectionnées AWS Config pour enregistrement.

Si vous exécutez des charges de travail éphémères, il se peut que vous constatiez une activité accrue d' AWS Config en raison de l'enregistrement des changements de configuration associés à la création et à la suppression de ces ressources temporaires. Une charge de travail éphémère est une utilisation temporaire des ressources informatiques chargées et exécutées si nécessaire.

Les exemples incluent les instances Spot Amazon Elastic Compute Cloud (Amazon EC2), les jobs Amazon EMR et. AWS Auto Scaling Si vous souhaitez éviter l'augmentation de l'activité liée à l'exécution de charges de travail éphémères, vous pouvez configurer l'enregistreur de configuration pour exclure l'enregistrement de ces types de ressources, ou exécuter ces types de charges de travail dans un compte distinct en désactivant pour éviter d' AWS Config augmenter l'enregistrement des configurations et l'évaluation des règles.

Considerations: All resource types with customizable overrides

Types de ressources enregistrés au niveau mondial | Les clusters globaux Aurora sont initialement inclus dans l'enregistrement

Le type de `AWS::RDS::GlobalCluster` ressource sera enregistré dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé.

Si vous ne souhaitez pas enregistrer `AWS::RDS::GlobalCluster` dans toutes les régions activées, choisissez « AWS RDS GlobalCluster », puis choisissez l'option « Exclure de l'enregistrement ».

Types de ressources mondiales | Les types de ressources IAM sont initialement exclus de l'enregistrement

Les types de ressources IAM globaux sont initialement exclus de l'enregistrement afin de vous aider à réduire les coûts. Cela inclut les utilisateurs, les groupes et les rôles IAM, ainsi que les politiques gérées par le client. Choisissez Supprimer pour supprimer l'exclusion et inclure ces ressources dans votre enregistrement.

L'exception concerne l'est des États-Unis (Virginie du Nord). Les types de ressources IAM enregistrés au niveau mondial sont initialement inclus dans la région USA Est (Virginie du Nord), car cette région fonctionne comme la région d'origine des types de ressources IAM mondiales.

En outre, les types de ressources IAM globaux (`AWS::IAM::User`, `AWS::IAM::Group``AWS::IAM::Role`, et`AWS::IAM::Policy`) ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Restrictions

Vous pouvez ajouter jusqu'à 100 exclusions de fréquence et 600 exclusions d'exclusion.

L'enregistrement quotidien ne prend pas en charge les types de ressources suivants :

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Disponibilité dans les régions

Avant de spécifier un type de ressource AWS Config à suivre, vérifiez la couverture des ressources par région disponible pour voir si le type de ressource est pris en charge dans la AWS région où vous l'avez configuré AWS Config. Si un type de ressource est pris AWS Config en charge par au moins une région, vous pouvez activer l'enregistrement de ce type de ressource dans toutes les régions prises en charge AWS Config, même si le type de ressource spécifié n'est pas pris en charge dans la AWS région où vous l'avez configuré AWS Config.

Restrictions

Aucune limite si tous les types de ressources ont la même fréquence. Vous pouvez ajouter jusqu'à 100 types de ressources avec une fréquence quotidienne si au moins un type de ressource est défini sur Continu.

La fréquence quotidienne n'est pas prise en charge pour les types de ressources suivants :

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Gouvernance des données

- Pour la période de conservation des données, choisissez la période de conservation par défaut pour conserver les AWS Config données pendant 7 ans (2557) ou définissez une période de conservation personnalisée pour les éléments enregistrés par. AWS Config

  AWS Config vous permet de supprimer vos données en spécifiant une période de conservation pour votre`ConfigurationItems`. Lorsque vous spécifiez une période de conservation, AWS Config elle conserve `ConfigurationItems` la vôtre pendant cette période spécifiée. Vous pouvez choisir une période comprise entre un minimum de 30 jours et un maximum de 7 ans (2557

jours). AWS Config supprime les données antérieures à la période de conservation que vous avez spécifiée.

- Pour le rôle IAM pour AWS Config, choisissez soit un rôle AWS Config lié à un service existant, soit un rôle IAM a depuis votre compte.
  - Les rôles liés à un service sont prédéfinis par AWS Config et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services.

> **Note**
>
> Recommandé : utilisez le rôle lié à un service
> Il est recommandé d'utiliser le rôle lié à un service. Un rôle lié à un service ajoute toutes les autorisations nécessaires AWS Config pour fonctionner comme prévu.

  - Sinon, choisissez un rôle IAM parmi l'un de vos rôles et politiques d'autorisation préexistants.

> **Note**
>
> Politiques d'autorisation pour les accès AWS Organizations Can Prevent
> Si vous utilisez un rôle IAM préexistant, assurez-vous qu'aucune politique d'autorisation ne vous AWS Config empêche AWS Organizations d'avoir l'autorisation d'enregistrer vos ressources. Pour plus d'informations sur les politiques d'autorisation pour AWS Organizations, consultez la section Gestion des politiques AWS Organizations dans le Guide de AWS Organizations l'utilisateur.
> Conservez le minimum d'autorisations lors de la réutilisation d'un rôle IAM
> Si vous utilisez un AWS service qui utilise AWS Config, tel que AWS Security Hub ou AWS Control Tower, et qu'un rôle IAM a déjà été créé, assurez-vous que le rôle IAM que vous utilisez lors de la configuration AWS Config conserve les mêmes autorisations minimales que le rôle IAM préexistant. Vous devez le faire pour vous assurer que l'autre AWS service continue de fonctionner comme prévu.
> Par exemple, si AWS Control Tower un rôle IAM permet de AWS Config lire des objets S3, assurez-vous que les mêmes autorisations sont accordées au rôle IAM que vous utilisez lors de la configuration. AWS Config Sinon, cela pourrait interférer avec le AWS Control Tower fonctionnement.

Mode de remise

- Pour le Mode de remise, choisissez le compartiment S3 auquel AWS Config envoie les fichiers d'historique de configuration et d'instantané de configuration :
  - Créer un compartiment : saisissez le nom de votre compartiment S3 dans le champ Nom du compartiment S3.

    Le nom que vous saisissez doit être unique parmi tous les noms de compartiment existants dans Amazon S3. Afin de garantir cette unicité, vous pouvez ajouter un préfixe, par exemple le nom de votre organisation. Une fois le nom du compartiment créé, vous ne pouvez plus le modifier. Pour plus d'informations, consultez Limites et restrictions applicables aux compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.
  - Choisir un compartiment de votre compte : choisissez votre compartiment préféré dans le champ Nom du compartiment S3.
  - Choisir un compartiment d'un autre compte : saisissez le nom du compartiment dans le champ Nom du compartiment S3.

    > **Note**
    >
    > Autorisations du bucket
    > Si vous choisissez un compartiment provenant d'un autre compte, ce compartiment doit être doté de politiques accordant des autorisations d'accès à AWS Config. Pour plus d'informations, consultez Autorisations pour le compartiment Amazon S3 pour le canal AWS Config de diffusion.
- Pour la rubrique Amazon SNS, choisissez Diffuser les modifications de configuration et les notifications dans une rubrique Amazon SNS pour envoyer des notifications telles que la livraison de l'historique de configuration, la livraison des instantanés de configuration et la conformité. AWS Config
- Si vous avez choisi de AWS Config diffuser sur un sujet Amazon SNS, choisissez le sujet cible :
  - Créer une rubrique : saisissez le nom de votre rubrique SNS dans le champ Nom de la rubrique.
  - Choisir une rubrique de votre compte : sélectionnez votre rubrique préférée dans le champ Nom de la rubrique.
  - Choisir la rubrique d'un autre compte : saisissez l'Amazon Resource Name (ARN) de la rubrique dans le champ ARN de la rubrique. Si vous choisissez un sujet depuis un autre compte, le sujet

doit être soumis à des politiques accordant des autorisations d'accès à AWS Config. Pour plus d'informations, consultez Autorisations relatives à la rubrique Amazon SNS.

> **Note**
>
> Région pour la rubrique Amazon SNS
> La rubrique Amazon SNS doit exister dans la même région que la région dans laquelle vous l'avez configurée. AWS Config

Règles

Si vous effectuez la configuration AWS Config dans une région qui prend en charge les règles, choisissez Next. Pour plus d'informations, consultez Ajouter, mettre à jour et supprimer des AWS Config règles.

Sinon, choisissez Confirmer.

Vérification

Vérifiez les détails AWS Config de votre configuration. Vous pouvez revenir en arrière pour modifier les changements apportés à chaque section. Choisissez Confirmer pour terminer la configuration AWS Config.

Pour plus d'informations

Pour plus d'informations sur la recherche des ressources existantes de votre compte et la compréhension de la configuration de vos ressources, consultez Affichage des configurations de ressource et de l'historique.

Vous pouvez également utiliser Amazon Simple Queue Service pour surveiller les AWS ressources par programmation. Pour plus d'informations, consultez Surveillance des modifications AWS des ressources avec Amazon SQS.

Configuration à l' AWS Config aide du AWS CLI

AWS CLI Il s'agit d'un outil unifié pour gérer vos AWS services. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs AWS services depuis la ligne de commande et utiliser des scripts pour les automatiser. Pour plus d'informations sur les AWS CLI outils AWS CLI et pour obtenir

des instructions sur leur installation, reportez-vous à ce qui suit dans le guide de AWS Command Line Interface l'utilisateur.

- AWS Command Line Interface Guide de l'utilisateur
- Préparation de l'installation de l' AWS Command Line Interface

Si nécessaire, entrez `aws configure` pour configurer le AWS CLI afin d'utiliser une AWS région AWS Config disponible.

Configuration

Consultez les rubriques suivantes pour configurer AWS Config le AWS CLI.

Rubriques

- Prérequis
- En AWS Config commençant par le AWS CLI
- Vérifier que le démarrage AWS Config a bien été effectué à l'aide du AWS CLI

Prérequis

Avant de procéder à la configuration AWS avec le AWS CLI, vous devez créer un compartiment Amazon S3, une rubrique Amazon SNS et un rôle IAM avec des politiques associées comme conditions préalables. Vous pouvez ensuite utiliser le AWS CLI pour spécifier le compartiment, le sujet et le rôle pour AWS Config. Suivez cette procédure pour configurer les conditions préalables pour AWS Config.

Table des matières

- Création d'un compartiment Amazon S3
- Création d'une rubrique Amazon SNS
- Création d'un rôle IAM

Création d'un compartiment Amazon S3

Si vous avez déjà un compartiment Amazon S3 dans votre compte et si vous voulez l'utiliser, ignorez cette étape et passez à l'étape Création d'une rubrique Amazon SNS.

Utilisation de la console S3

Pour créer un compartiment

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Dans Nom du compartiment, saisissez un nom compatible DNS pour votre compartiment.

   Le nom du compartiment doit présenter les caractéristiques suivantes :

   - Il doit être unique sur l'ensemble d'Amazon S3.
   - Il doit comporter entre 3 et 63 caractères.
   - Ne contient pas de majuscules.
   - Il doit commencer par une minuscule ou un chiffre.

   Une fois le compartiment créé, vous ne pouvez pas changer son nom. Vérifiez que le nom de compartiment que vous choisissez n'existe pas déjà parmi tous les noms de compartiment existant dans Amazon S3. Pour plus d'informations sur les règles et les conventions de dénomination de compartiment, consultez Limites et restrictions applicables aux compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

   > **Important**
   >
   > Évitez d'inclure des informations sensibles dans le nom du compartiment. Le nom de compartiment est visible dans les URL qui pointent vers les objets du compartiment.

4. Dans Région, choisissez la AWS région dans laquelle vous souhaitez que le bucket réside.

   Choisissez une Région proche de vous afin de limiter la latence et les coûts, et répondre aux exigences légales. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste des AWS régions Amazon S3, consultez la section Points AWS de terminaison de service dans le Référence générale d'Amazon Web Services.

5. Dans Paramètres de compartiment pour Bloquer l'accès public, choisissez les paramètres de blocage de l'accès public que vous souhaitez appliquer au compartiment.

Nous vous recommandons de laisser tous les paramètres activés, sauf si vous savez que vous devez en désactiver un ou plusieurs d'entre eux pour votre cas d'utilisation, par exemple pour héberger un site web public. Les paramètres de blocage de l'accès public que vous activez pour le compartiment seront également activés pour tous les points d'accès que vous créez dans le compartiment. Pour plus d'informations sur le blocage de l'accès public, consultez Utilisation de la fonctionnalité de blocage de l'accès public Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

6. (Facultatif) Si vous souhaitez activer la fonctionnalité de verrouillage d'objet S3 :

   a. Choisissez Paramètres avancés et lisez le message qui s'affiche.

   > **Important**
   >
   > Vous ne pouvez activer la fonctionnalité de verrouillage d'objet S3 pour un compartiment que lors de sa création. Si vous activez le verrouillage d'objet pour le compartiment, vous ne pouvez pas le désactiver ultérieurement. L'activation du verrouillage d'objet active également la gestion des versions pour le compartiment. Après avoir activé le verrouillage d'objet pour le compartiment, vous devez configurer les paramètres de la fonctionnalité de verrouillage d'objet avant que les objets du compartiment ne soient protégés. Pour plus d'informations sur la configuration de la protection des objets, consultez Configuration du verrouillage d'objet S3 à l'aide de la console Amazon S3.

   b. Si vous souhaitez activer la fonctionnalité de verrouillage d'objet, entrez activer dans la zone de texte et choisissez Confirmer.

   Pour plus d'informations sur la fonctionnalité de verrouillage d'objet S3, consultez Verrouillage d'objets à l'aide de la fonctionnalité de verrouillage d'objet Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

7. Choisissez Créer un compartiment.

Utilisation des AWS SDK

Lorsque vous utilisez les AWS SDK pour créer un compartiment, vous devez créer un client, puis utiliser le client pour envoyer une demande de création d'un compartiment. En tant que bonne pratique, vous devez créer votre client et votre compartiment dans la même Région AWS. Si vous ne

spécifiez pas de Région lorsque vous créez un client ou un compartiment, Amazon S3 utilise USA Est (Virginie du Nord), la Région par défaut.

Pour créer un client permettant d'accéder à un point de terminaison à double pile, vous devez spécifier un Région AWS. Pour plus d'informations, consultez Points de terminaison Amazon S3 Dual-Stack. Pour obtenir la liste des régions disponibles Régions AWS, consultez la section Régions et points de terminaison dans le Références générales AWS.

Lorsque vous créez un client, la Région est mappée au point de terminaison spécifique à la Région. Le client utilise ce point de terminaison pour communiquer avec Amazon S3 : `s3.<region>.amazonaws.com`. Si votre Région a été lancée après le 20 mars 2019, votre client et votre compartiment doivent se trouver dans la même Région. Par conséquent, vous pouvez utiliser un client dans la Région USA Est (Virginie du Nord) pour créer un compartiment dans n'importe quelle Région lancée avant le 20 mars 2019. Pour plus d'informations, consultez Points de terminaison hérités.

Ces exemples de code AWS SDK exécutent les tâches suivantes :

- Créer un client en indiquant explicitement une Région AWS – Dans l'exemple, le client utilise le point de terminaison `s3.us-west-2.amazonaws.com` pour communiquer avec Amazon S3. Vous pouvez spécifier n'importe quelle Région AWS. Pour en obtenir la liste Régions AWS, voir Régions et points de terminaison dans le manuel de référence AWS général.
- Envoyer une demande de création de compartiment en indiquant uniquement un nom de compartiment — Le client envoie une demande à Amazon S3 pour créer le compartiment dans la Région où vous avez créé un client.
- Récupérer des informations relatives à l'emplacement du compartiment – Amazon S3 stocke les informations relatives à l'emplacement du compartiment dans la sous-ressource de l'emplacement associée au compartiment.

Les exemples de code suivants montrent comment utiliser`CreateBucket`.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

Créez un compartiment avec le verrouillage des objets activé.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS SDK for .NET API.

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
```

```
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi
```

```
  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS CLI commandes.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
bool AwsDoc::S3::CreateBucket(const Aws::String &bucketName,
                              const Aws::Client::ClientConfiguration
 &clientConfig) {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    //TODO(user): Change the bucket location constraint enum to your target
 Region.
    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                       clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: CreateBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    }
    else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS SDK for C++ API.

CLI

AWS CLI

Exemple 1 : pour créer un bucket

L'`create-bucket`exemple suivant crée un compartiment nommé `my-bucket` :

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1
```

Sortie :

```
{
    "Location": "/my-bucket"
}
```

Pour plus d'informations, consultez la section Création d'un compartiment dans le guide de l'utilisateur Amazon S3.

Exemple 2 : pour créer un bucket avec le propriétaire imposé

L'`create-bucket`exemple suivant crée un bucket nommé `my-bucket` qui utilise le paramètre imposé par le propriétaire du bucket pour S3 Object Ownership.

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Sortie :

```
{
    "Location": "/my-bucket"
}
```

Pour plus d'informations, veuillez consulter la rubrique Contrôle de la propriété des objets et désactivation des listes ACL dans le Guide de l'utilisateur Amazon S3.

Exemple 3 : Pour créer un bucket en dehors de la région ``us-east-1``

L'`create-bucket`exemple suivant crée un compartiment nommé `my-bucket` dans la `eu-west-1` région. Les régions situées en dehors de `us-east-1` doivent être spécifiées afin de créer le compartiment dans la région souhaitée. `LocationConstraint`

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Sortie :

```
{
    "Location": "http://my-bucket.s3.amazonaws.com/"
}
```

Pour plus d'informations, consultez la section Création d'un compartiment dans le guide de l'utilisateur Amazon S3.

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS CLI commandes.

Go

Kit SDK for Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
```

```
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(name string, region string) error {
 _, err := basics.S3Client.CreateBucket(context.TODO(), &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  log.Printf("Couldn't create bucket %v in Region %v. Here's why: %v\n",
   name, region, err)
 }
 return err
}
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS SDK for Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez un compartiment.

```
import software.amazon.awssdk.core.waiters.WaiterResponse;
```

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketResponse;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.s3.waiters.S3Waiter;
import java.net.URISyntaxException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateBucket {
    public static void main(String[] args) throws URISyntaxException {
        final String usage = """

                Usage:
                    <bucketName>\s

                Where:
                    bucketName - The name of the bucket to create. The bucket
 name must be unique, or an error occurs.
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String bucketName = args[0];
        System.out.format("Creating a bucket named %s\n", bucketName);
        Region region = Region.US_EAST_1;
        S3Client s3 = S3Client.builder()
                .region(region)
                .build();

        createBucket(s3, bucketName);
```

```
        s3.close();
    }

    public static void createBucket(S3Client s3Client, String bucketName) {
        try {
            S3Waiter s3Waiter = s3Client.waiter();
            CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            s3Client.createBucket(bucketRequest);
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            // Wait until the bucket is created and print out the response.
            WaiterResponse<HeadBucketResponse> waiterResponse =
 s3Waiter.waitUntilBucketExists(bucketRequestWait);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println(bucketName + " is ready");

        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

Créez un compartiment avec le verrouillage des objets activé.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
 bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();

        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
```

```
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créer le compartiment.

```
import { CreateBucketCommand, S3Client } from "@aws-sdk/client-s3";

const client = new S3Client({});

export const main = async () => {
  const command = new CreateBucketCommand({
    // The name of the bucket. Bucket names are unique and have several other
 constraints.
    // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
    Bucket: "bucket-name",
  });

  try {
    const { Location } = await client.send(command);
    console.log(`Bucket created with location ${Location}`);
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- Pour de plus amples informations, consultez le Guide du développeur AWS SDK for JavaScript.
- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section AWS SDK pour la référence de l'API Kotlin.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez un compartiment.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
$exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS SDK for PHP API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créer un compartiment avec les paramètres par défaut.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

Créer un compartiment soumis à la gestion des versions avec une configuration de cycle de vie.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
```

```
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
 expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- Pour plus de détails sur l'API, consultez CreateBucketle AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require "aws-sdk-s3"

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      "None. You must create a bucket before you can get its location!"
    else
```

```
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("doc-example-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section Référence des AWS SDK for Ruby API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
pub async fn create_bucket(
    client: &Client,
    bucket_name: &str,
    region: &str,
) -> Result<CreateBucketOutput, SdkError<CreateBucketError>> {
    let constraint = BucketLocationConstraint::from(region);
```

```
    let cfg = CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await
}
```

- Pour plus de détails sur l'API, voir CreateBucketla section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    TRY.
        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
        ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section de référence du AWS SDK pour l'API SAP ABAP.

Swift

Kit SDK pour Swift

> **Note**
>
> Ceci est une documentation préliminaire pour une fonctionnalité en version de prévisualisation. Elle est susceptible d'être modifiée.

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
public func createBucket(name: String) async throws {
    let config = S3ClientTypes.CreateBucketConfiguration(
        locationConstraint: .usEast2
    )
    let input = CreateBucketInput(
        bucket: name,
        createBucketConfiguration: config
    )
    _ = try await client.createBucket(input: input)
}
```

- Pour plus de détails sur l'API, reportez-vous CreateBucketà la section AWS SDK pour la référence de l'API Swift.

> **Note**
>
> Vous pouvez également utiliser un compartiment Amazon S3 d'un autre compte, mais vous devrez peut-être créer une politique pour le compartiment qui accorde des autorisations d'accès à AWS Config. Pour en savoir plus sur l'accord d'autorisations à un compartiment Amazon S3, consultez Autorisations pour le compartiment Amazon S3 pour le canal AWS Config de diffusion, puis passer à Création d'une rubrique Amazon SNS.

Création d'une rubrique Amazon SNS

Si vous avez déjà une rubrique Amazon SNS dans votre compte et que vous souhaitez l'utiliser, ignorez cette étape et passez à Création d'un rôle IAM.

Utilisation de la console SNS

Pour créer une rubrique Amazon SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Effectuez l'une des actions suivantes :
   - Si aucun sujet n'a encore été créé sous votre Compte AWS nom, lisez la description d'Amazon SNS sur la page d'accueil.
   - Si des sujets ont déjà été créés sous votre Compte AWS nom, dans le panneau de navigation, sélectionnez Sujets.
3. Sur la page Rubriques, choisissez Créer une rubrique.
4. Sur la page Créer une rubrique, dans la section Détails, procédez comme suit :
   a. Pour Type, choisissez un type de rubrique (Standard ou FIFO).
   b. Entrez un Nom pour la rubrique. Pour une rubrique FIFO, ajoutez .fifo à la fin du nom.
   c. (Facultatif) Entrez un Nom d'affichage pour votre rubrique.
   d. (Facultatif) Pour une rubrique FIFO, vous pouvez choisir déduplication des messages basée sur le contenu pour activer la déduplication des messages par défaut. Pour plus d'informations, consultez Déduplication de message pour les rubriques FIFO.
5. (Facultatif) Développez la section Chiffrement et effectuez les opérations suivantes. Pour plus d'informations, consultez Chiffrement au repos.
   a. Choisissez Activer le chiffrement.
   b. Spécifiez la clé principale client (CMK). Pour plus d'informations, veuillez consulter la rubrique Termes clés.

      Pour chaque type de CMK, les champs Description, Compte et CARN CMK s'affichent.

> **Important**
>
> Si vous n'êtes pas le propriétaire de la clé CMK, ou si vous vous connectez avec un compte n'ayant pas les autorisations `kms:ListAliases` et `kms:DescribeKey`, vous ne pouvez pas afficher les informations relatives au CMK sur la console Amazon SNS.
> Demandez au propriétaire du CMK de vous accorder ces autorisations. Pour plus d'informations, consultez Autorisations d'API AWS KMS : référence des actions et ressources dans le Guide du développeur AWS Key Management Service .

- La clé CMK AWS gérée pour Amazon SNS (par défaut) alias/aws/sns est sélectionnée par défaut.

  > **Note**
  >
  > Gardez à l'esprit les points suivants :
  >
  > - La première fois que vous utilisez le AWS Management Console pour spécifier la clé CMK AWS gérée pour Amazon SNS pour un sujet AWS KMS , la clé CMK gérée pour Amazon SNS est créée AWS .
  > - Sinon, la première fois que vous utilisez l'`Publish`action sur un sujet pour lequel SSE est activé, la clé CMK AWS gérée est AWS KMS créée pour Amazon SNS.

- Pour utiliser une clé CMK personnalisée à partir de votre clé CMK Compte AWS, choisissez le champ Clé principale du client (CMK), puis choisissez la clé CMK personnalisée dans la liste.

  > **Note**
  >
  > Pour obtenir des instructions pour la création de CMK personnalisées, consultez Création de clés dans le Guide du développeur AWS Key Management Service .

- Pour utiliser un ARN CMK personnalisé provenant de votre compte Compte AWS ou d'un autre AWS compte, saisissez-le dans le champ Clé principale du client (CMK).

6. (Facultatif) Par défaut, seul le propriétaire de la rubrique peut publier dans la rubrique ou s'abonner à la rubrique. Pour configurer des autorisations d'accès supplémentaires, développez la section Politique d'accès. Pour plus d'informations, consultez Gestion des identités et des accès dans Amazon SNS et Cas d'exemple pour le contrôle d'accès Amazon SNS.

   > **Note**
   >
   > Lorsque vous créez une rubrique à l'aide de la console, la politique par défaut utilise la clé de condition `aws:SourceOwner`. Cette clé est similaire à `aws:SourceAccount`.

7. (Facultatif) Pour configurer la façon dont Amazon SNS retente la distribution des messages en échec, développez la section Politique de nouvelle tentative de distribution (HTTP/S). Pour plus d'informations, consultez Nouvelle tentative de distribution des messages Amazon SNS.
8. (Facultatif) Pour configurer la manière dont Amazon SNS enregistre la livraison des messages CloudWatch, développez la section Enregistrement de l'état de livraison. Pour plus d'informations, voir État de distribution des messages Amazon SNS.
9. (Facultatif) Pour ajouter des balises de métadonnées à la rubrique, développez la section Balises, saisissez une clé et une valeur (facultatif) et choisissez Ajouter une balise. Pour plus d'informations, consultez Identification des rubriques Amazon SNS.
10. Choisissez Créer une rubrique.

    Le sujet est créé et la ***MyTopic***page s'affiche.

    Le Nom de la rubrique, l'ARN, (facultatif) le Nom d'affichage et l'ID de compte AWS du Propriétaire de la rubrique sont affichés dans la section Détails.

11. Copiez l'ARN de rubrique dans le Presse-papiers, par exemple :

    ```
    arn:aws:sns:us-east-2:123456789012:MyTopic
    ```

Pour abonner une adresse e-mail à la rubrique Amazon SNS

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Dans le volet de navigation de gauche, choisissez Abonnements.
3. Sur la page Abonnements, choisissez Créer un abonnement.
4. Sur la page Créer un abonnement, dans la section Détails, procédez comme suit :

a. Pour ARN de rubrique, choisissez l'ARN (Amazon Resource Name) d'une rubrique.

b. Pour Protocole, choisissez un type de point de terminaison. Les types de point de terminaison disponibles sont les suivants :

- HTTP/HTTPS
- E-mail/E-mail-JSON
- Amazon Data Firehose
- Amazon SQS

> **Note**
>
> Pour vous abonner à une Rubrique SNS FIFO, choisissez cette option.

- AWS Lambda
- Point de terminaison de l'application de plateforme
- SMS

c. Pour Point de terminaison, saisissez la valeur du point de terminaison, telle qu'une adresse e-mail ou l'ARN d'une file d'attente Amazon SQS.

d. Points de terminaison Firehose uniquement : pour l'ARN du rôle d'abonnement, spécifiez l'ARN du rôle IAM que vous avez créé pour écrire dans les flux de diffusion Firehose. Pour plus d'informations, consultez la section Conditions préalables à l'abonnement des flux de diffusion Firehose aux rubriques Amazon SNS.

e. (Facultatif) Pour les points de terminaison Firehose, Amazon SQS et HTTP/S, vous pouvez également activer la livraison de messages bruts. Pour plus d'informations, consultez Remise des messages bruts Amazon SNS.

f. (Facultatif) Pour configurer une politique de filtre, développez la section Politique de filtre d'abonnement. Pour plus d'informations, consultez les politiques de filtre d'abonnement Amazon SNS.

g. (Facultatif) Pour configurer une file d’attente de lettres mortes pour l’abonnement, développez la section Politique de reconduite (File d’attente de lettres mortes). Pour plus d'informations, consultez Files d'attente de lettres mortes d'Amazon SNS.

h. Choisissez Créer un abonnement.

   La console crée l'abonnement et ouvre la page Détails de l’abonnement.

Utilisation des AWS SDK

Pour utiliser un AWS SDK, vous devez le configurer avec vos informations d'identification. Pour plus d'informations, consultez Les fichiers de configuration et d'informations d'identification partagés dans le AWS Guide de référence des kits SDK et des outils.

Les exemples de code suivants montrent comment utiliser`CreateTopic`.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez une rubrique avec un nom spécifique.

```
using System;
using System.Threading.Tasks;
using Amazon.SimpleNotificationService;
using Amazon.SimpleNotificationService.Model;

/// <summary>
/// This example shows how to use Amazon Simple Notification Service
/// (Amazon SNS) to add a new Amazon SNS topic.
/// </summary>
public class CreateSNSTopic
{
    public static async Task Main()
    {
        string topicName = "ExampleSNSTopic";

        IAmazonSimpleNotificationService client = new
AmazonSimpleNotificationServiceClient();

        var topicArn = await CreateSNSTopicAsync(client, topicName);
        Console.WriteLine($"New topic ARN: {topicArn}");
    }
```

```
        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Créez une nouvelle rubrique avec un nom et des attributs FIFO et de déduplication spécifiques.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };
```

```
        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }

            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
"true");
            }
        }

        var createResponse = await
_amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS SDK for .NET API.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
```

```
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS SDK for C++ API.

CLI

AWS CLI

Pour créer une rubrique SNS

L'exemple `create-topic` suivant crée une rubrique SNS nommée `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Sortie :

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

Pour plus d'informations, consultez la section Utilisation de l'interface de ligne de AWS commande avec Amazon SQS et Amazon SNS dans le Guide de l'utilisateur de AWS l'interface de ligne de commande.

- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS CLI commandes.

Go

Kit SDK for Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
```

```
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(topicName string, isFifoTopic bool,
 contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(context.TODO(), &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS SDK for Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }
```

```
        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le client dans un module séparé et exportez-le.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

Importez le kit SDK et les modules client et appelez l'API.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- Pour de plus amples informations, consultez le AWS SDK for JavaScript Guide du développeur.
- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS SDK for JavaScript API.

Kotlin

SDK pour Kotlin

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section AWS SDK pour la référence de l'API Kotlin.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
```

```
use Aws\Sns\SnsClient;


/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- Pour de plus amples informations, consultez le Guide du développeur AWS SDK for PHP.
- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS SDK for PHP API.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- Pour plus de détails sur l'API, consultez CreateTopicle AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = "YourTopicName" # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
```

```
  unless sns_topic_creator.create_topic(topic_name)
    puts "The topic was not created. Stopping program."
    exit 1
  end
end
```

- Pour de plus amples informations, consultez le Guide du développeur AWS SDK for Ruby.
- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section Référence des AWS SDK for Ruby API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- Pour plus de détails sur l'API, voir CreateTopicla section de référence de l'API AWS SDK for Rust.

SAP ABAP

Kit SDK pour SAP ABAP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   TRY.
       oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
is returned for testing purposes. "
       MESSAGE 'SNS topic created' TYPE 'I'.
     CATCH /aws1/cx_snstopiclimitexcdex.
       MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- Pour plus de détails sur l'API, reportez-vous CreateTopicà la section de référence du AWS SDK pour l'API SAP ABAP.

> **Note**
>
> Vous pouvez également utiliser une rubrique Amazon SNS appartenant à un autre compte, mais, dans ce cas, vous devrez créer une politique qui accorde des autorisations d'accès à AWS Config. Pour en savoir plus sur l'octroi d'autorisations à une rubrique Amazon SNS, consultez Autorisations relatives à la rubrique Amazon SNS, puis passez à Création d'un rôle IAM.

Création d'un rôle IAM

Utilisation de la console IAM

Vous pouvez utiliser la console IAM pour créer un rôle IAM qui accorde des AWS Config autorisations pour accéder à votre compartiment Amazon S3, accéder à votre rubrique Amazon SNS et obtenir les détails de configuration des ressources prises en charge. AWS Lorsque vous utilisez la console

pour créer un rôle IAM, AWS Config attache automatiquement les autorisations requises au rôle pour vous.

> **Note**
>
> Si vous avez utilisé un AWS service qui utilise AWS Config (tel que AWS Security Hub ou AWS Control Tower) et qu'un AWS Config rôle a déjà été créé, vous devez vous assurer que le rôle IAM que vous utilisez lors de la configuration AWS Config conserve les mêmes privilèges minimaux que le AWS Config rôle déjà créé afin que l'autre AWS service continue de fonctionner comme prévu.
> Par exemple, si AWS Control Tower possède un rôle IAM qui permet de lire AWS Config les objets Amazon S3, vous devez garantir que les mêmes autorisations sont accordées dans le rôle IAM que vous utilisez lors de la configuration. AWS Config Dans le cas contraire, cela pourrait interférer avec les opérations de la tour de AWS contrôle.
> Pour plus d'informations sur les rôles IAM pour AWS Config, consultez AWS Identity and Access Management.

Pour créer un rôle pour un AWS service

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de la console IAM, sélectionnez Roles (Rôles), puis Create role (Créer un rôle).
3. Pour Sélectionner une entité de confiance, choisissez Service AWS .
4. Choisissez le cas d'utilisation que vous souhaitez pour AWS Config : Config - Customizable, Config - Organizations, Config ou Config - Conformance Packs. Ensuite, choisissez Suivant.
5. Sur la page Nommer, vérifier et créer, passez en revue les détails relatifs à votre rôle et choisissez Créer un rôle.

Utilisation des AWS SDK

Pour utiliser un AWS SDK, vous devez le configurer avec vos informations d'identification. Pour plus d'informations, consultez Les fichiers de configuration et d'informations d'identification partagés dans le AWS Guide de référence des kits SDK et des outils.

Les exemples de code suivants montrent comment utiliser`CreateRole`.

.NET

AWS SDK for .NET

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS SDK for .NET API.

Bash

AWS CLI avec le script Bash

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
```

```
  echo "  -n role_name   The name of the IAM role."
  echo "  -p policy_json -- The assume role policy document."
  echo ""
}

# Retrieve the calling parameters.
while getopts "n:p:h" option; do
  case "${option}" in
    n) role_name="${OPTARG}" ;;
    p) policy_document="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$role_name" ]]; then
  errecho "ERROR: You must provide a role name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$policy_document" ]]; then
  errecho "ERROR: You must provide a policy document with the -p parameter."
  usage
  return 1
fi

response=$(aws iam create-role \
  --role-name "$role_name" \
  --assume-role-policy-document "$policy_document" \
  --output text \
  --query Role.Arn)

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
```

```
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS CLI commandes.

C++

SDK pour C++

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
```

```
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS SDK for C++ API.

CLI

AWS CLI

Exemple 1 : Pour créer un rôle IAM

La commande `create-role` suivante crée un rôle nommé `Test-Role` et lui attache une politique d'approbation.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Sortie :

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

La politique d'approbation est définie sous la forme d'un document JSON dans le fichier Test-Role-Trust-Policy.json. (Le nom et l'extension du fichier n'ont aucune importance.) La politique d'approbation doit spécifier un principal.

Pour attacher une politique des autorisations à un rôle, utilisez la commande `put-role-policy`.

Pour plus d'informations, consultez Création de rôles IAM dans le Guide de l'utilisateur AWS IAM.

Exemple 2 : Pour créer un rôle IAM avec une durée de session maximale spécifiée

La commande `create-role` suivante crée un rôle nommé `Test-Role` et définit une durée de session maximale de 7 200 secondes (2 heures).

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

Sortie :

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Pour plus d'informations, consultez la section Modification de la durée maximale de session (AWS API) d'un rôle dans le guide de l'utilisateur AWS IAM.

Exemple 3 : Pour créer un rôle IAM avec des balises

La commande suivante crée un rôle IAM `Test-Role` avec des balises. Cet exemple utilise l'indicateur de paramètre `--tags` avec les balises au format JSON suivantes : `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. L'indicateur `--tags` peut également être utilisé avec des balises au format raccourci : `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Sortie :

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
```

```
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

Pour plus d'informations, veuillez consulter Étiquette de rôles IAM dans le Guide de l'utilisateur AWS IAM.

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS CLI commandes.

Go

Kit SDK for Go V2

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
```

```
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(roleName string, trustedUserArn string)
 (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version:   "2012-10-17",
  Statement: []PolicyStatement{{
   Effect: "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action: []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(context.TODO(),
 &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
}
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS SDK for Go API.

Java

SDK pour Java 2.x

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
```

```
                    fileLocation - The location of the JSON document that
represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }

    public static Object readJsonSimpleDemo(String filename) throws Exception {
```

```
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS SDK for Java 2.x API.

JavaScript

SDK pour JavaScript (v3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

Créez le rôle.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
```

```
        },
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS SDK for JavaScript API.

PHP

Kit SDK pour PHP

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
```

```
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS SDK for PHP API.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple crée un nouveau rôle nommé **`MyNewRole`** et y attache la politique trouvée dans le fichier**`NewRoleTrustPolicy.json`**. Notez que vous devez utiliser le paramètre **`-Raw`** switch pour traiter correctement le fichier de politique JSON. Le document de politique affiché dans la sortie est codé en URL. Il est décodé dans cet exemple à l'aide de la méthode **`UrlDecode`** .NET.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Sortie :

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
```

```
                              %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                              %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                              %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                              %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                              %20%5D%0D%0A%7D
CreateDate                  : 4/15/2015 11:04:23 AM
Path                        : /
RoleId                      : V5PAJI2KPN4EAEXAMPLE1
RoleName                    : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- Pour plus de détails sur l'API, consultez CreateRolele AWS manuel de référence de l'API SDK for Python (Boto3).

Ruby

Kit SDK pour Ruby

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
     )
   end

   role_arn
 rescue Aws::IAM::Errors::ServiceError => e
   @logger.error("Error creating role: #{e.message}")
   nil
 end
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section Référence des AWS SDK for Ruby API.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- Pour plus de détails sur l'API, voir CreateRolela section de référence de l'API AWS SDK for Rust.

Swift

Kit SDK pour Swift

> **Note**
>
> Ceci est une documentation préliminaire pour une fonctionnalité en version de prévisualisation. Elle est susceptible d'être modifiée.

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
   public func createRole(name: String, policyDocument: String) async throws ->
String {
       let input = CreateRoleInput(
           assumeRolePolicyDocument: policyDocument,
           roleName: name
       )
       do {
           let output = try await client.createRole(input: input)
           guard let role = output.role else {
               throw ServiceHandlerError.noSuchRole
           }
           guard let id = role.roleId else {
               throw ServiceHandlerError.noSuchRole
           }
           return id
       } catch {
           throw error
       }
   }
```

- Pour plus de détails sur l'API, reportez-vous CreateRoleà la section AWS SDK pour la référence de l'API Swift.

En AWS Config commençant par le AWS CLI

> **Note**
>
> Avant de procéder à la configuration AWS Config avec le AWS CLI, vous devez créer un compartiment S3, un sujet SNS et un rôle IAM avec des politiques associées comme conditions préalables. Vous pouvez ensuite utiliser le AWS CLI pour spécifier le compartiment, le sujet et le rôle pour AWS Config. Pour configurer vos prérequis pour AWS Config, consultez la section Conditions préalables.

Pour AWS Config commencer AWS CLI, utilisez les commandes put-configuration-recorder, put-delivery-channel et start-configuration-recorder, comme suit :

- La commande `put-configuration-recorder` crée un nouvel enregistreur de configuration pour enregistrer les configurations de ressources spécifiées.
- La commande `put-delivery-channel` crée un objet de canal de livraison pour fournir des informations de configuration à un compartiment S3 et à une rubrique SNS.
- Une fois qu'un canal de livraison est créé, `start-configuration-recorder` commence à enregistrer les configurations de ressources que vous avez sélectionnées, lesquelles sont affichées dans votre compte AWS .

> **Note**
>
> Un seul enregistreur de configuration et un seul canal de livraison par région peut être appliqué à chaque région AWS de votre compte.

Vous pouvez spécifier le nom de l'enregistreur et le nom de ressource Amazon (ARN) du rôle IAM assumé AWS Config et utilisé par l'enregistreur de configuration. AWS Config attribue automatiquement le nom « par défaut » lors de la création de l'enregistreur de configuration. Vous ne pouvez pas modifier le nom de l'enregistreur de configuration après sa création. Pour modifier le nom de l'enregistreur de configuration, vous devez le supprimer et en créer un autre en lui attribuant un nouveau nom.

AWS Config Pour configurer l'agrégation de données multicomptes et multirégions avec le AWS CLI, voir Configuration d'un agrégateur à l'aide de l'interface de AWS ligne de commande. Vous devez

créer un enregistreur de configuration distinct pour chaque région dans Compte AWS laquelle vous souhaitez enregistrer des éléments de configuration.

Table des matières

- put-configuration-recorder
- put-delivery-channel
- start-configuration-recorder

put-configuration-recorder

Votre commande `put-configuration-recorder` devrait ressembler à l'exemple suivant.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Cette commande utilise les `---recording-group` champs `--configuration-recorder` et.

> **Note**
>
> Groupe d'enregistrement et enregistreur de configuration
> Le champ `--recording-group` indique les types de ressources enregistrés.
> Le `--configuration-recorder` champ indique `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

Groupe d'enregistrement

`put-configuration-recorder` utilise les options suivantes pour le paramètre `--recording-group` :

- `allSupported=true`— AWS Config enregistre les modifications de configuration pour tous les types de ressources pris en charge, à l'exception des types de ressources IAM globaux. Lorsque AWS Config la prise en charge d'un nouveau type de ressource est ajoutée, commence AWS Config automatiquement à enregistrer les ressources de ce type.

- `includeGlobalResourceTypes=true` : cette option concerne uniquement les types de ressource IAM mondiales : utilisateurs, groupes et rôles IAM, et politiques gérées par le client. Ces types de ressources IAM globaux ne peuvent être enregistrés que AWS Config dans les régions où ils AWS Config étaient disponibles avant février 2022. Vous ne pouvez pas enregistrer les types de ressources IAM globaux dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

> **Important**
>
> Les clusters globaux Aurora sont enregistrés dans toutes les régions activées
> Le type de `AWS::RDS::GlobalCluster` ressource sera enregistré dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé, même s'il `includeGlobalResourceTypes` est défini sur`false`. L'option `includeGlobalResourceTypes` s'applique uniquement aux utilisateurs, aux groupes et aux rôles IAM, ainsi qu'aux politiques gérées par le client.
> Si vous ne souhaitez pas enregistrer `AWS::RDS::GlobalCluster` dans toutes les régions activées, utilisez l'une des politiques d'enregistrement suivantes :
>
> 1. Enregistrer tous les types de ressources actuels et futurs avec des exclusions (`EXCLUSION_BY_RESOURCE_TYPES`), ou
> 2. Enregistrer des types de ressources spécifiques (`INCLUSION_BY_RESOURCE_TYPES`).
>
> Pour plus d'informations, consultez Sélection des ressources qui sont enregistrées.

> **Important**
>
> inclusion GlobalResourceTypes et stratégie d'enregistrement des exclusions
> Le `includeGlobalResourceTypes` champ n'a aucun impact sur la stratégie `EXCLUSION_BY_RESOURCE_TYPES` d'enregistrement. Cela signifie que les types de ressources IAM globaux (utilisateurs IAM, groupes, rôles et politiques gérées par le client) ne seront pas automatiquement ajoutés en tant qu'exclusions pour le `exclusionByResourceTypes` moment `includeGlobalResourceTypes` défini sur. `false`
> Le `includeGlobalResourceTypes` champ ne doit être utilisé que pour modifier le `AllSupported` champ, car le champ par défaut est d'enregistrer les `AllSupported` modifications de configuration pour tous les types de ressources pris en charge, à l'exception des types de ressources IAM globaux. Pour inclure les types de

ressources IAM globaux lorsqu'il `AllSupported` est défini sur`true`, assurez-vous de `includeGlobalResourceTypes` définir `true` sur.
Pour exclure les types de ressources IAM globaux pour la stratégie `EXCLUSION_BY_RESOURCE_TYPES` d'enregistrement, vous devez les ajouter manuellement `resourceTypes` dans le champ de`exclusionByResourceTypes`.

> **Note**
>
> Champs obligatoires et facultatifs
> Avant de définir `includeGlobalResourceTypes` sur `true`, définissez le champ `allSupported` sur `true`.
> Vous pouvez éventuellement définir le champ `useOnly` de `RecordingStrategy` sur `ALL_SUPPORTED_RESOURCE_TYPES` (facultatif).

> **Note**
>
> Champs de remplacement
> Si vous définissez cette `includeGlobalResourceTypes` option`false`, mais que vous listez les types de ressources IAM globaux dans le `resourceTypes` champ de RecordingGroup, les modifications de configuration pour les types de ressources spécifiés AWS Config seront toujours enregistrées, que vous ayez défini le `includeGlobalResourceTypes` champ sur false ou non.
> Si vous ne souhaitez pas enregistrer les changements de configuration apportés aux types de ressources IAM enregistrés au niveau mondial (utilisateurs, groupes et rôles IAM, ainsi que les politiques gérées par le client), veillez à ne pas les répertorier dans le champ `resourceTypes` si le champ `includeGlobalResourceTypes` est défini sur false.

- `recordingStrategy` : indique la politique d'enregistrement appliqué à l'enregistreur de configuration. Le fichier `recordingGroup.json` spécifie les types de ressources qui seront enregistrés par AWS Config :
  - Si vous définissez le `useOnly` champ sur`ALL_SUPPORTED_RESOURCE_TYPES`, AWS Config enregistre les modifications de RecordingStrategyconfiguration pour tous les types de ressources pris en charge, à l'exception des types de ressources IAM globaux. Vous pouvez éventuellement définir le `allSupported` champ de RecordingGroupà`true`. Lorsque AWS Config la prise en

charge d'un nouveau type de ressource est ajoutée, commence AWS Config automatiquement à enregistrer les ressources de ce type.

- Si vous définissez le `useOnly` champ de RecordingStrategyà`INCLUSION_BY_RESOURCE_TYPES`, AWS Config enregistre les modifications de configuration uniquement pour les types de ressources que vous spécifiez dans le `resourceTypes` champ de RecordingGroup.
- Si vous définissez le `useOnly` champ RecordingStrategyà`EXCLUSION_BY_RESOURCE_TYPES`, AWS Config enregistre les modifications de configuration pour tous les types de ressources pris en charge, à l'exception des types de ressources que vous spécifiez comme devant être exclus de l'enregistrement dans le `resourceTypes` champ de ExclusionByResourceTypes.

> **Note**
>
> Champs obligatoires et facultatifs
>
> Le champ `recordingStrategy` est facultatif lorsque vous définissez le champ `allSupported` de `--recording-group` sur `true`.
>
> Le champ `recordingStrategy` est facultatif lorsque vous répertoriez les types de ressources dans le champ `resourceTypes` de `--recording-group`.
>
> Le champ `recordingStrategy` est obligatoire si vous répertoriez les types de ressources à exclure de l'enregistrement dans le champ `resourceTypes` de `exclusionByResourceTypes`.

> **Note**
>
> Champs de remplacement
>
> Si vous choisissez `EXCLUSION_BY_RESOURCE_TYPES` pour la politique d'enregistrement, le champ `exclusionByResourceTypes` remplacera les autres propriétés de la requête. Par exemple, même si vous définissez `includeGlobalResourceTypes` sur false, les types de ressources IAM enregistrés au niveau mondial seront toujours enregistrés automatiquement dans cette option, sauf si ces types de ressources sont spécifiquement répertoriés en tant qu'exemptions dans le champ `resourceTypes` de `exclusionByResourceTypes`.

> **Note**
>
> Types de ressources globales et politique d'enregistrement des exclusions de ressources
> Par défaut, si vous choisissez la stratégie `EXCLUSION_BY_RESOURCE_TYPES` d'enregistrement, when AWS Config ajoute la prise en charge d'un nouveau type de ressource dans la région où vous avez configuré l'enregistreur de configuration, y compris les types de ressources globaux, AWS Config commence à enregistrer automatiquement les ressources de ce type.
> Sauf mention contraire dans la liste des exclusions, ils `AWS::RDS::GlobalCluster` seront enregistrés automatiquement dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé.
> Les utilisateurs, les groupes, les rôles et les politiques gérées par le client IAM seront enregistrés dans la région dans laquelle vous avez configuré l'enregistreur de configuration s'il s'agit d'une région disponible avant février 2022. AWS Config Vous ne pouvez pas enregistrer les types de ressources IAM globaux dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Voici la syntaxe de la demande pour `recordingGroup.json`.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

> **Note**
>
> Politiques d'autorisation pour les accès AWS Organizations Can Prevent

Si vous utilisez un rôle IAM préexistant, assurez-vous qu'aucune politique d'autorisation ne vous AWS Config empêche AWS Organizations d'avoir l'autorisation d'enregistrer vos ressources. Pour plus d'informations sur les politiques d'autorisation pour AWS Organizations, consultez la section Gestion des politiques AWS Organizations dans le Guide de AWS Organizations l'utilisateur.

Conservez le minimum d'autorisations lors de la réutilisation d'un rôle IAM

Si vous utilisez un AWS service qui utilise AWS Config, tel que AWS Security Hub ou AWS Control Tower, et qu'un rôle IAM a déjà été créé, assurez-vous que le rôle IAM que vous utilisez lors de la configuration AWS Config conserve les mêmes autorisations minimales que le rôle IAM préexistant. Vous devez le faire pour vous assurer que l'autre AWS service continue de fonctionner comme prévu.

Par exemple, si AWS Control Tower un rôle IAM permet de AWS Config lire des objets S3, assurez-vous que les mêmes autorisations sont accordées au rôle IAM que vous utilisez lors de la configuration. AWS Config Sinon, cela pourrait interférer avec le AWS Control Tower fonctionnement.

Note

Nombre élevé d' AWS Config évaluations

Vous remarquerez peut-être une augmentation de l'activité de votre compte lors de votre premier mois d'enregistrement avec AWS Config par rapport aux mois suivants. Au cours du processus de démarrage initial, AWS Config exécute des évaluations sur toutes les ressources de votre compte que vous avez sélectionnées AWS Config pour enregistrement.

Si vous exécutez des charges de travail éphémères, vous constaterez peut-être une augmentation de l'activité en raison de AWS Config l'enregistrement des modifications de configuration associées à la création et à la suppression de ces ressources temporaires. Une charge de travail éphémère est une utilisation temporaire des ressources informatiques chargées et exécutées si nécessaire. Les exemples incluent les instances Spot Amazon Elastic Compute Cloud (Amazon EC2), les jobs Amazon EMR et. AWS Auto Scaling Si vous souhaitez éviter l'augmentation de l'activité liée à l'exécution de charges de travail éphémères, vous pouvez configurer l'enregistreur de configuration pour exclure l'enregistrement de ces types de ressources, ou exécuter ces types de charges de travail dans un compte distinct en désactivant pour éviter d' AWS Config augmenter l'enregistrement des configurations et l'évaluation des règles.

> **Note**
>
> Disponibilité dans les régions
>
> Avant de spécifier un type de ressource AWS Config à suivre, vérifiez la couverture des ressources par région disponible pour voir si le type de ressource est pris en charge dans la AWS région dans laquelle vous configurez AWS Config. Si un type de ressource est pris AWS Config en charge par au moins une région, vous pouvez activer l'enregistrement de ce type de ressource dans toutes les régions prises en charge AWS Config, même si le type de ressource spécifié n'est pas pris en charge dans la AWS région dans laquelle vous configurez AWS Config.

Enregistreur de configuration

`put-configuration-recorder` utilise les champs suivants pour le paramètre `--configuration-recorder` :

- `name`— Nom de l'enregistreur de configuration. AWS Config attribue automatiquement le nom « par défaut » lors de la création de l'enregistreur de configuration.
- `roleARN`— Amazon Resource Name (ARN) du rôle IAM assumé AWS Config et utilisé par l'enregistreur de configuration.
- `recordingMode`— Spécifie la fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration. AWS Config prend en charge l'enregistrement continu et l'enregistrement quotidien. L'enregistrement en continu vous permet d'enregistrer les modifications de configuration en continu, chaque fois qu'un changement a lieu. L'enregistrement quotidien vous permet de recevoir un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il diffère de l'élément de configuration enregistré précédemment.
  - `recordingFrequency`— Fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration.

> **Note**
>
> AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

- `recordingModeOverrides` : ce champ vous permet de définir vos exclusions pour le mode d'enregistrement. Il s'agit d'un tableau d'objets `recordingModeOverride`. Chaque objet `recordingModeOverride` du tableau `recordingModeOverrides` comprend trois champs :
  - `description` : description que vous fournissez pour l'exclusion.
  - `recordingFrequency` : fréquence d'enregistrement qui sera appliquée à tous les types de ressources spécifiés dans l'exclusion.
  - `resourceTypes`— Une liste séparée par des virgules qui indique les types de ressources AWS Config inclus dans la dérogation.

> **Note**
>
> Champs obligatoires et facultatifs
>
> Le champ `recordingMode` pour `put-configuration-recorder` est facultatif. Par défaut, la fréquence d'enregistrement de l'enregistreur de configuration est définie sur Enregistrement en continu.

> **Note**
>
> Restrictions
>
> L'enregistrement quotidien ne prend pas en charge les types de ressources suivants :
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Pour la stratégie d'enregistrement Enregistrer tous les types de ressources actuels et futurs pris en charge (`ALL_SUPPORTED_RESOURCE_TYPES`), ces types de ressources seront définis sur Enregistrement en continu.

Le `configurationRecorder.json` fichier spécifie `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

put-delivery-channel

Les exemples de code suivants montrent comment utiliser`PutDeliveryChannel`.

CLI

AWS CLI

Pour créer un canal de diffusion

La commande suivante fournit les paramètres du canal de diffusion sous forme de code JSON :

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Le `deliveryChannel.json` fichier spécifie les attributs du canal de diffusion :

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Cet exemple définit les attributs suivants :

`name`- Le nom du canal de diffusion. Par défaut, AWS Config attribue le nom `default` à un nouveau canal de distribution. Vous ne pouvez pas mettre à jour le nom du canal de distribution avec la commande. `put-delivery-channel` Pour connaître les étapes à suivre pour modifier le nom, voir Renommer le canal de diffusion. `s3BucketName` - Le nom du compartiment Amazon S3 auquel AWS Config fournit des instantanés de configuration et des fichiers d'historique de configuration. Si vous spécifiez un compartiment appartenant à un autre AWS compte, ce compartiment doit disposer de politiques accordant des autorisations d'accès à Config. AWS Pour de plus d'informations, consultez Autorisations pour le compartiment Amazon S3.

`snsTopicARN`- Le nom de ressource Amazon (ARN) de la rubrique Amazon SNS à laquelle AWS Config envoie des notifications concernant les modifications de configuration. Si vous choisissez un sujet depuis un autre compte, le sujet doit comporter des politiques accordant des autorisations d'accès à Config. AWS Pour plus d'informations, consultez la rubrique Autorisations pour Amazon SNS.

`configSnapshotDeliveryProperties`- Contient l'`deliveryFrequency`attribut, qui définit la fréquence à laquelle AWS Config fournit des instantanés de configuration et la fréquence à laquelle il invoque des évaluations pour les règles de configuration périodiques.

Si la commande aboutit, AWS Config ne renvoie aucune sortie. Pour vérifier les paramètres de votre canal de diffusion, exécutez la describe-delivery-channels commande.

- Pour plus de détails sur l'API, voir PutDeliveryCanal dans AWS CLI Command Reference.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple modifie la propriété DeliveryFrequency d'un canal de diffusion existant.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Pour plus de détails sur l'API, consultez la section PutDeliveryChannel in AWS Tools for PowerShell Cmdlet Reference.

start-configuration-recorder

Pour terminer l'activation AWS Config, utilisez la `start-configuration-recorder`commande.

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Vérifier que le démarrage AWS Config a bien été effectué à l'aide du AWS CLI

Après avoir démarré AWS Config, vous pouvez utiliser des AWS CLI commandes pour vérifier que le AWS Config est en cours d'exécution et que cela AWS Config a créé un enregistreur de configuration et un canal de diffusion. Vous pouvez également confirmer que AWS Config l'enregistrement et la transmission des configurations au canal de diffusion ont commencé.

Table des matières

- Vérifier que le canal de livraison a été créé
- Vérifier que l'enregistreur de configuration a été créé
- Vérifiez que l'enregistrement AWS Config a commencé

Vérifier que le canal de livraison a été créé

Utilisez la commande `describe-delivery-channels` pour vérifier que votre compartiment Amazon S3 et votre rubrique Amazon SNS sont configurés.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

Lorsque vous utilisez la CLI, l'API du service ou les SDK pour configurer votre canal de diffusion et que vous ne spécifiez pas de nom, le nom « » `default` est AWS Config automatiquement attribué.

Vérifier que l'enregistreur de configuration a été créé

Utilisez la commande `describe-configuration-recorders` pour vérifier qu'un enregistreur de configuration est créé et qu'il a endossé un rôle IAM. Pour plus d'informations, consultez Création d'un rôle IAM.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Vérifiez que l'enregistrement AWS Config a commencé

Utilisez la `describe-configuration-recorder-status`commande pour vérifier que l'enregistrement des configurations des AWS ressources prises en charge existant dans votre compte AWS Config a commencé. Les configurations enregistrées sont fournies au canal de livraison spécifié.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
```

```
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

La valeur `true` dans le champ `recording` confirme que l'enregistreur de configuration a commencé l'enregistrement des configurations de toutes vos ressources. AWS Config enregistre l'heure au format UTC. La sortie est affichée sous forme d'horodatage Unix.

Pour des informations sur la recherche des ressources existantes de votre compte et la compréhension de la configuration de vos ressources, veuillez consulter la page Affichage des configurations de ressource et de l'historique.

Utilisation AWS Config avec un AWS SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque SDK fournit une API, des exemples de code et de la documentation qui facilitent la création d'applications par les développeurs dans leur langage préféré.

Documentation SDK	Exemples de code
AWS SDK for C++	AWS SDK for C++ exemples de code
AWS CLI	AWS CLI exemples de code
AWS SDK for Go	AWS SDK for Go exemples de code
AWS SDK for Java	AWS SDK for Java exemples de code
AWS SDK for JavaScript	AWS SDK for JavaScript exemples de code
Kit AWS SDK pour Kotlin	Kit AWS SDK pour Kotlin exemples de code

Documentation SDK	Exemples de code
AWS SDK for .NET	AWS SDK for .NET exemples de code
AWS SDK for PHP	AWS SDK for PHP exemples de code
AWS Tools for PowerShell	Outils pour des exemples PowerShell de code
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemples de code
AWS SDK for Ruby	AWS SDK for Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code
Kit AWS SDK pour Swift	Kit AWS SDK pour Swift exemples de code

Exemple de disponibilité

Vous n’avez pas trouvé ce dont vous avez besoin ? Demandez un exemple de code en utilisant le lien Faire un commentaire en bas de cette page.

Gestion de l'enregistreur de configuration

AWS Config utilise l'enregistreur de configuration pour détecter les modifications apportées à la configuration de vos ressources et capturer ces modifications sous forme d'éléments de configuration. Vous devez créer un enregistreur de configuration avant de AWS Config pouvoir suivre la configuration de vos ressources. Lorsque vous démarrez l'enregistreur de configuration, AWS Config il fait l'inventaire de toutes les AWS ressources de votre compte.

Vous ne pouvez avoir qu'un seul canal d'enregistrement de configuration par AWS Compte AWS région et le canal de diffusion doit être utilisé AWS Config.

Si vous effectuez la configuration à AWS Config l'aide de la console ou de la AWS CLI, l'enregistreur de configuration est AWS Config automatiquement créé puis démarré pour vous. Pour plus d'informations, consultez Commencer avec AWS Config.

Par défaut, l'enregistreur de configuration enregistre toutes les ressources prises en charge dans la région où AWS Config est en cours d'exécution. Vous pouvez créer un enregistreur de configuration personnalisé qui enregistre uniquement les types de ressource que vous indiquez. Pour plus d'informations, consultez AWS Ressources d'enregistrement.

Des frais d'utilisation du service vous sont facturés lorsque vous AWS Config commencez à enregistrer des configurations. Pour de plus amples informations sur la tarification, veuillez consulter AWS Config Pricing (français non garanti).

> **Important**
>
> Les résultats de l'évaluation des ressources supprimées peuvent être conservés si l'enregistreur de configuration est désactivé
> Si l'enregistreur de configuration est désactivé, il désactive la possibilité de AWS Config suivre les modifications apportées à la configuration de vos ressources, y compris leurs suppressions. Cela signifie que vous pouvez voir les résultats de l'évaluation des ressources précédemment supprimées si vous désactivez l'enregistreur de configuration.

Gestion de l'enregistreur de configuration (console)

Vous pouvez utiliser la AWS Config console pour arrêter ou démarrer l'enregistreur de configuration. Vous pouvez également modifier la fréquence d'enregistrement de l'enregistreur de configuration.

To stop or start the configuration recorder

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Arrêter ou démarrer l'enregistreur de configuration :
   - Si vous souhaitez arrêter l'enregistrement, sous L'enregistrement est activé, choisissez Désactiver. À l'invite, choisissez Continuer.
   - Si vous souhaitez démarrer l'enregistrement, sous L'enregistrement est désactivé, choisissez Activer. À l'invite, choisissez Continuer.

To change the recording frequency

AWS Config prend en charge l'enregistrement continu et l'enregistrement quotidien. L'enregistrement en continu vous permet d'enregistrer les modifications de configuration en continu, chaque fois qu'un changement a lieu. L'enregistrement quotidien vous permet de recevoir un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il diffère de l'élément de configuration enregistré précédemment. Pour plus d'informations, consultez Fréquence d'enregistrement.

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Choisissez Modifier pour afficher les options sous « Fréquence d'enregistrement ».

Gestion de l'enregistreur de configuration (AWS CLI)

Vous pouvez utiliser le AWS CLI pour arrêter ou démarrer l'enregistreur de configuration. Vous pouvez également renommer ou supprimer l'enregistreur de configuration à l' AWS CLI aide de l' AWS Config API ou de l'un des AWS SDK. Les étapes suivantes vous aident à utiliser l' AWS CLI.

To stop the configuration recorder

Utilisez la commande `stop-configuration-recorder` :

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

To start the configuration recorder

Utilisez la commande `start-configuration-recorder` :

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

To change the recording frequency

Utilisez la commande `put-configuration-recorder` pour modifier la fréquence d'enregistrement de l'enregistreur de configuration :

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

Le `configurationRecorder.json` fichier spécifie `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

`put-configuration-recorder` utilise les champs suivants pour le paramètre `--configuration-recorder` :

- `name`— Nom de l'enregistreur de configuration. AWS Config attribue automatiquement le nom « par défaut » lors de la création de l'enregistreur de configuration.
- `roleARN`— Amazon Resource Name (ARN) du rôle IAM assumé AWS Config et utilisé par l'enregistreur de configuration.
- `recordingMode`— Spécifie la fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration. AWS Config prend en charge l'enregistrement continu et l'enregistrement quotidien. L'enregistrement en continu vous permet d'enregistrer les modifications de configuration en continu, chaque fois qu'un changement a lieu. L'enregistrement quotidien vous permet de recevoir un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il diffère de l'élément de configuration enregistré précédemment.
  - `recordingFrequency`— Fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration.

    > **Note**
    >
    > AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

  - `recordingModeOverrides` : ce champ vous permet de définir vos exclusions pour le mode d'enregistrement. Il s'agit d'un tableau d'objets `recordingModeOverride`. Chaque objet `recordingModeOverride` du tableau `recordingModeOverrides` comprend trois champs :
    - `description` : description que vous fournissez pour l'exclusion.
    - `recordingFrequency` : fréquence d'enregistrement qui sera appliquée à tous les types de ressources spécifiés dans l'exclusion.
    - `resourceTypes`— Liste séparée par des virgules qui indique les types de ressources AWS Config inclus dans la dérogation.

> **Note**
>
> Champs obligatoires et facultatifs

Le champ `recordingMode` pour `put-configuration-recorder` est facultatif. Par défaut, la fréquence d'enregistrement de l'enregistreur de configuration est définie sur Enregistrement en continu.

> **Note**
>
> Restrictions
>
> L'enregistrement quotidien ne prend pas en charge les types de ressources suivants :
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Pour la stratégie d'enregistrement Enregistrer tous les types de ressources actuels et futurs pris en charge (`ALL_SUPPORTED_RESOURCE_TYPES`), ces types de ressources seront définis sur Enregistrement en continu.

To delete the configuration recorder

Utilisez la commande `delete-configuration-recorder` :

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To rename the configuration recorder

Pour modifier le nom de l'enregistreur de configuration, vous devez le supprimer et en créer un nouveau avec le nom souhaité.

1. Utilisez la commande `describe-configuration-recorders` pour rechercher le nom de votre enregistreur de configuration actuel :

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
```

```
            "name": "default"
        }
    ]
}
```

2. Utilisez la commande `delete-configuration-recorder` pour arrêter l'enregistreur de configuration actuel :

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. Utilisez la commande `put-configuration-recorder` pour créer un enregistreur de configuration avec le nom souhaité :

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Utilisez la commande `start-configuration-recorder` pour reprendre l'enregistrement :

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Détection des dérives de l'enregistreur de configuration

Le type de ressource `AWS::Config::ConfigurationRecorder` est un élément de configuration (CI) pour l'enregistreur de configuration qui suit toutes les modifications apportées à l'état de l'enregistreur de configuration. Vous pouvez utiliser ce CI pour vérifier si l'état de l'enregistreur de configuration est différent ou s'il a dérivé de son état précédent. Par exemple, ce CI suit si des mises à jour ont été apportées aux types de ressources que vous avez autorisés AWS Config à suivre, si vous avez arrêté ou démarré l'enregistreur de configuration, ou si vous avez supprimé ou désinstallé l'enregistreur de configuration. Un enregistreur de configuration dérivé indique que vous ne détectez pas avec précision les modifications apportées aux types de ressources souhaités. Si votre enregistreur de configuration a dérivé, il peut induire des faux négatifs ou des faux positifs dans les résultats de conformité.

Le type de `AWS::Config::ConfigurationRecorder` ressource est un type de ressource système AWS Config et l'enregistrement de ce type de ressource est activé par défaut dans toutes les régions prises en charge. L'enregistrement du type de ressource `AWS::Config::ConfigurationRecorder` est effectué sans frais supplémentaires.

Gestion du canal de livraison

Comme il enregistre AWS Config en permanence les modifications apportées à vos AWS ressources, il envoie des notifications et des états de configuration mis à jour via le canal de livraison. Vous pouvez gérer le canal de diffusion pour contrôler l'endroit où les mises à jour de configuration sont AWS Config envoyées.

Vous ne pouvez avoir qu'un seul canal de livraison par AWS région et par région Compte AWS, et le canal de livraison doit être utilisé AWS Config.

Lorsqu'une modification de configuration est AWS Config détectée pour une ressource et que la notification dépasse la taille maximale autorisée par Amazon SNS, elle inclut un bref résumé de l'élément de configuration. Vous pouvez consulter la notification complète dans l'emplacement de compartiment Amazon S3 spécifié dans le champ `s3BucketLocation`. Pour plus d'informations, consultez Exemple de notification de changement avec un élément de configuration trop grand.

> **Note**
>
> AWS Config prend en charge AWS KMS le chiffrement pour les compartiments Amazon S3 utilisés par AWS Config
>
> Vous pouvez fournir une clé AWS Key Management Service (AWS KMS) ou un alias Amazon Resource Name (ARN) pour chiffrer les données transmises à votre compartiment Amazon Simple Storage Service (Amazon S3). Par défaut, AWS Config fournit l'historique de configuration et les fichiers instantanés à votre compartiment Amazon S3 et chiffre les données au repos à l'aide du chiffrement S3 AES-256 côté serveur, SSE-S3. Toutefois, si vous fournissez AWS Config votre clé KMS ou votre alias ARN, AWS Config utilise cette clé KMS au lieu du chiffrement AES-256.
>
> AWS Config ne prend pas en charge le canal de diffusion vers un compartiment Amazon S3 où le verrouillage des objets est activé avec la rétention par défaut activée. Pour plus d'informations, consultez Utilisation du verrouillage des objets S3.

Rubriques

- Terminologie
- Mise à jour du canal de livraison
- Renommer les canaux de livraison
- Composants d'un élément de configuration

- Fournir des instantanés de configuration à un compartiment Amazon S3
- Notifications envoyées par AWS Config à une rubrique Amazon SNS

Terminologie

Un élément de configuration représente une point-in-time vue des différents attributs d'une AWS ressource prise en charge qui existe dans votre compte. Les composants d'un élément de configuration incluent les métadonnées, les attributs, les relations, la configuration actuelle et les événements connexes. AWS Config crée un élément de configuration chaque fois qu'il détecte une modification d'un type de ressource qu'il enregistre. Par exemple, si vous AWS Config enregistrez des compartiments Amazon S3, AWS Config crée un élément de configuration chaque fois qu'un compartiment est créé, mis à jour ou supprimé. Vous pouvez également sélectionner de AWS Config créer un élément de configuration à la fréquence d'enregistrement que vous avez définie.

Un historique de configuration est un ensemble d'éléments de configuration pour une ressource donnée sur une période donnée. Il permet de répondre aux questions concernant, par exemple, la date de création de la ressource, la configuration de la ressource au cours du dernier mois, ainsi que les changements de configuration effectués hier à 9h. L'historique de configuration est disponible dans plusieurs formats. AWS Config fournit automatiquement un fichier d'historique de configuration pour chaque type de ressource enregistré dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez sélectionner une ressource donnée dans la AWS Config console et accéder à tous les éléments de configuration précédents pour cette ressource à l'aide de la chronologie. En outre, vous pouvez accéder aux éléments de l'historique de configuration pour une ressource à partir de l'interface API.

Un instantané de configuration est un ensemble d'éléments de configuration pour les ressources prises en charge de votre compte. Cet instantané de la configuration est une image complète des ressources qui sont en cours d'enregistrement et de leur configuration. Il peut être un outil utile pour la validation de votre configuration. Par exemple, vous pouvez examiner l'instantané de configuration régulièrement pour les ressources qui sont configurées de façon incorrecte ou qui ne devraient pas exister. Il est disponible dans plusieurs formats. Vous pouvez faire en sorte que l'instantané de configuration soit diffusé vers un compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez. En outre, vous pouvez sélectionner un moment dans la AWS Config console et parcourir l'instantané des éléments de configuration à l'aide des relations entre les ressources.

Un flux de configuration est une liste automatiquement mise à jour de tous les éléments de configuration pour les ressources en cours AWS Config d'enregistrement. Chaque fois qu'une

ressource est créée, modifiée ou supprimée, AWS Config crée un élément de configuration et l'ajoute dans le flux de configuration. Le flux de configuration fonctionne en utilisant la rubrique Amazon Simple Notification Service (Amazon SNS) de votre choix. Le flux de configuration est utile pour observer les modifications de configuration au fur et à mesure qu'elles se produisent afin de détecter les problèmes potentiels, de générer des notifications si certaines ressources sont modifiées ou de mettre à jour les systèmes externes qui doivent refléter la configuration de vos AWS ressources.

Mise à jour du canal de livraison

Lorsque vous mettez à jour le canal de livraison, vous pouvez définir les options suivantes :

- Le compartiment Amazon S3 auquel AWS Config envoie les instantanés de configuration et les fichiers d'historique de configuration.
- À quelle fréquence AWS Config fournit des instantanés de configuration à votre compartiment Amazon S3.
- Rubrique Amazon SNS à laquelle les notifications relatives aux modifications de configuration sont AWS Config envoyées.

Pour mettre à jour le canal de diffusion (console)

Vous pouvez utiliser la AWS Config console pour définir le compartiment Amazon S3 et la rubrique Amazon SNS pour votre canal de diffusion. Pour savoir comment gérer ces paramètres, consultez Configuration à l' AWS Config aide de la console.

La console n'autorise pas les options à renommer le canal de livraison, à régler la fréquence pour les instantanés de configuration ou à supprimer le canal de livraison. Pour effectuer ces tâches, vous devez utiliser l' AWS CLI AWS Config API ou l'un des AWS SDK.

Pour mettre à jour le canal de diffusion (AWS SDK)

Les exemples de code suivants montrent comment utiliser`PutDeliveryChannel`.

CLI

AWS CLI

Pour créer un canal de diffusion

La commande suivante fournit les paramètres du canal de diffusion sous forme de code JSON :

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Le `deliveryChannel.json` fichier spécifie les attributs du canal de diffusion :

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Cet exemple définit les attributs suivants :

`name`- Le nom du canal de diffusion. Par défaut, AWS Config attribue le nom `default` à un nouveau canal de distribution. Vous ne pouvez pas mettre à jour le nom du canal de distribution avec la commande. `put-delivery-channel` Pour connaître les étapes à suivre pour modifier le nom, voir Renommer le canal de diffusion. `s3BucketName` - Le nom du compartiment Amazon S3 auquel AWS Config fournit des instantanés de configuration et des fichiers d'historique de configuration. Si vous spécifiez un compartiment appartenant à un autre AWS compte, ce compartiment doit disposer de politiques accordant des autorisations d'accès à Config. AWS Pour de plus d'informations, consultez Autorisations pour le compartiment Amazon S3.

`snsTopicARN`- Le nom de ressource Amazon (ARN) de la rubrique Amazon SNS à laquelle AWS Config envoie des notifications concernant les modifications de configuration. Si vous choisissez un sujet depuis un autre compte, le sujet doit comporter des politiques accordant des autorisations d'accès à Config. AWS Pour plus d'informations, consultez la rubrique Autorisations pour Amazon SNS.

`configSnapshotDeliveryProperties`- Contient l'`deliveryFrequency`attribut, qui définit la fréquence à laquelle AWS Config fournit des instantanés de configuration et la fréquence à laquelle il invoque des évaluations pour les règles de configuration périodiques.

Si la commande aboutit, AWS Config ne renvoie aucune sortie. Pour vérifier les paramètres de votre canal de diffusion, exécutez la describe-delivery-channels commande.

- Pour plus de détails sur l'API, voir PutDeliveryCanal dans AWS CLI Command Reference.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple modifie la propriété DeliveryFrequency d'un canal de diffusion existant.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Pour plus de détails sur l'API, consultez la section PutDeliveryChannel in AWS Tools for PowerShell Cmdlet Reference.

(Facultatif) Vous pouvez utiliser la commande `describe-delivery-channels` pour vérifier que les paramètres du canal de livraison sont à jour :

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

Les exemples de code suivants montrent comment utiliser`DescribeDeliveryChannels`.

CLI

AWS CLI

Pour obtenir des informations sur le canal de livraison

La commande suivante renvoie des informations sur le canal de diffusion :

```
aws configservice describe-delivery-channels
```

Sortie :

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Pour plus de détails sur l'API, consultez la section DescribeDeliveryCanaux dans AWS CLI Command Reference.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple extrait le canal de distribution de la région et affiche les détails.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Sortie :

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Pour plus de détails sur l'API, consultez la section DescribeDeliveryChannels in AWS Tools for PowerShell Cmdlet Reference.

Renommer les canaux de livraison

Pour modifier le nom du canal de livraison, vous devez le supprimer et en créer un nouveau avec le nom souhaité. Avant de pouvoir supprimer le canal de livraison, vous devez temporairement arrêter l'enregistreur de configuration.

La AWS Config console n'offre pas la possibilité de supprimer le canal de diffusion. Vous devez donc utiliser la AWS CLI, l' AWS Config API ou l'un des AWS SDK.

Pour renommer le canal de livraison (AWS CLI)

Renommer le canal de diffusion à l'aide du AWS CLI

1. Utilisez la commande `stop-configuration-recorder` pour arrêter l'enregistreur de configuration :

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. Utilisez la commande `describe-delivery-channels` et notez les attributs de votre canal de livraison :

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. Utilisez la commande `delete-delivery-channel` pour supprimer le canal de livraison :

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Utilisez la commande `put-delivery-channel` pour créer un canal de livraison avec le nom souhaité :

```
$ aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Le fichier deliveryChannel.json spécifie les attributs du canal de livraison :

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Utilisez la commande `start-configuration-recorder` pour reprendre l'enregistrement :

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Composants d'un élément de configuration

Un élément de configuration représente une point-in-time vue des différents attributs d'une AWS ressource prise en charge qui existe dans votre compte. Les composants d'un élément de configuration incluent les métadonnées, les attributs, les relations, la configuration actuelle et les événements connexes. AWS Config crée un élément de configuration chaque fois qu'il détecte une modification d'un type de ressource qu'il enregistre. Par exemple, si vous AWS Config enregistrez des compartiments Amazon S3, AWS Config crée un élément de configuration chaque fois qu'un compartiment est créé, mis à jour ou supprimé. Vous pouvez également sélectionner de AWS Config créer un élément de configuration à la fréquence d'enregistrement que vous avez définie.

Un élément de configuration comporte les composants ci-dessous.

Composant	Description	Contains
Metadonnées	Informations sur cet élément de configuration	• ID de version • Heure de capture de l'élément de configuration • Statut de l'élément de configuration indiquant si l'élément a été capturé avec succès • ID d'état indiquant l'ordre des éléments de configuration d'une ressource
Attributs	Attributs de ressource	• ID de ressource • Liste des balises clé-valeur de cette ressource • Type de ressource (voirTypes de ressource pris en charge) • Amazon Resource Name (ARN) • Zone de disponibilité qui contient cette ressource, le cas échéant • Heure de création de la ressource
Relations	Mode de liaison de la ressource aux autres ressources associées au compte	Description de la relation, par exemple : le volume Amazon EBS `vol-1234567` est attaché à une instance Amazon EC2 `i-a1b2c3d4`
Configuration actuelle	Informations retournées via un appel à l'API de description ou de liste de la ressource	Par exemple, l'API `DescribeVolumes` retourne les informations suivantes sur le volume : • Zone de disponibilité qui contient le volume • Heure à laquelle le volume a été attaché • ID de l'instance EC2 à laquelle le volume est attaché

Composant	Description	Contains
		• Statut actuel du volume • État du DeleteOnTermination drapeau • Périphérique auquel le volume est attaché • Type de volume, par exemple `gp2`, `io1`, `standard`

Remarques

1. Une relation d'élément de configuration n'inclut pas les dépendances de flux ou de flux de données de réseau. Les éléments de configuration ne peuvent pas être personnalisés pour représenter l'architecture de l'application.
2. Depuis la version 1.3, le champ relatedEvents est vide. Vous pouvez accéder à l'LookupEvents API dans la référence d'AWS CloudTrail API pour récupérer les événements relatifs à la ressource.
3. Depuis la version 1.3, le champ configurationItemMD5Hash est vide. Vous pouvez utiliser le configurationStateId champ pour vous assurer que vous disposez de l'élément de configuration le plus récent.

Fournir des instantanés de configuration à un compartiment Amazon S3

AWS Config fournit des instantanés de configuration des AWS ressources enregistrées AWS Config dans le compartiment Amazon S3 que vous avez spécifié lors de la configuration de votre canal de diffusion.

Rubriques

- Fourniture d'instantanés de configuration
- Exemple de capture instantanée de configuration à partir de AWS Config
- Vérification de l'état de diffusion
- Affichage de l'instantané de configuration dans un compartiment Amazon S3

Fourniture d'instantanés de configuration

AWS Config génère des instantanés de configuration lorsque vous appelez l'action DeliverConfigSnapshot ou que vous exécutez la AWS CLI `deliver-config-snapshot` commande. AWS Config stocke les instantanés de configuration dans le compartiment Amazon S3 que vous avez spécifié lors de l'activation AWS Config.

Tapez la `deliver-config-snapshot`commande en spécifiant le nom attribué AWS Config lors de la configuration de votre canal de diffusion, par exemple :

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

Exemple de capture instantanée de configuration à partir de AWS Config

Voici un exemple des informations AWS Config incluses dans un instantané de configuration. L'instantané décrit la configuration des ressources enregistrées AWS Config dans la région actuelle pour vous Compte AWS, ainsi que les relations entre ces ressources.

> **Note**
>
> L'instantané de configuration peut inclure des références à des types de ressources et ID de ressource qui ne sont pas pris en charge.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
```

```
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
```

```
        {
            "configurationItemVersion": "1.0",
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
```

```
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
```

```
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
```

```
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

L'étape suivante consiste à vérifier que l'instantané de cette configuration a été diffusé avec succès sur le canal de livraison.

Vérification de l'état de diffusion

Tapez la `describe-delivery-channel-status`commande pour vérifier que les configurations AWS Config ont commencé à être diffusées sur le canal de distribution spécifié, par exemple :

```
$ aws configservice describe-delivery-channel-status
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
```

```
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

La réponse répertorie l'état des trois formats de diffusion AWS Config utilisés pour fournir des configurations à votre compartiment et à votre sujet.

Observez le champ `lastSuccessfulTime` dans `configSnapshotDeliveryInfo`. Le temps doit correspondre à la dernière fois où vous avez demandé la diffusion de l'instantané de la configuration.

> **Note**
>
> AWS Config utilise le format UTC (temps universel coordonné) pour enregistrer l'heure.

Affichage de l'instantané de configuration dans un compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste de Tous les compartiments de la console Amazon S3, cliquez sur le nom de votre compartiment Amazon S3.
3. Cliquez sur les dossiers imbriqués dans votre compartiment jusqu'à ce que vous voyiez l'objet `ConfigSnapshot` avec un ID d'instantané qui correspond à celui retourné par la commande. Téléchargez et ouvrez l'objet pour afficher l'instantané de configuration.

Le compartiment S3 contient également un fichier vide nommé`ConfigWritabilityCheckFile`. AWS Config crée ce fichier pour vérifier que le service peut correctement écrire dans le compartiment S3.

Notifications envoyées par AWS Config à une rubrique Amazon SNS

> **Note**
>
> Avant de AWS Config pouvoir envoyer des notifications à une rubrique Amazon SNS, vous devez d'abord configurer l'enregistreur de configuration et le canal de diffusion. Pour plus d'informations, consultez Gestion de l'enregistreur de configuration et Gestion du canal de diffusion.

Vous pouvez configurer AWS Config pour diffuser les changements de configuration et les notifications vers une rubrique Amazon SNS. Par exemple, lorsqu'une ressource est mise à jour, une notification peut être envoyée à votre adresse e-mail pour que vous puissiez consulter les changements. Vous pouvez également être averti quand AWS Config évalue vos règles personnalisées ou gérées sur vos ressources. Pour plus d'informations, consultez la section Connexion et surveillance AWS Config.

AWS Config envoie des notifications pour les événements suivants :

- Changement d'élément de configuration pour une ressource.
- L'historique de configuration pour une ressource a été diffusé pour votre compte.
- Un instantané de configuration pour des ressources enregistrées a été a démarré et diffusé pour votre compte.
- État de conformité de vos ressources et si celles-ci sont conformes à vos règles.
- Evaluation démarrée pour une règle sur vos ressources.
- AWS Config n'a pas pu envoyer la notification à votre compte.

Rubriques

- Exemple de notification de changement d'élément de configuration

- Exemple de notification de diffusion de l'historique de configuration
- Exemple de notification de démarrage de la diffusion d'un instantané de configuration
- Exemple de notification de diffusion d'un instantané de configuration
- Exemple de notification de modification de conformité
- Exemple de notification d'une évaluation de règles démarrée
- Exemple de notification de changement avec un élément de configuration trop grand
- Exemple de notification d'échec de diffusion

Exemple de notification de changement d'élément de configuration

AWS Config utilise Amazon SNS pour envoyer des notifications aux points de terminaison d'abonnement. Ces notifications indiquent l'état de livraison des instantanés de configuration et des historiques de configuration, ainsi que chaque élément de configuration AWS Config créé lorsque les configurations des AWS ressources enregistrées changent. AWS Config envoie également des notifications indiquant si vos ressources sont conformes à vos règles. Si vous choisissez que les notifications vous soient envoyées par e-mail, vous pouvez utiliser des filtres dans votre application cliente de messagerie basés sur la ligne d'objet et le corps de message de l'e-mail.

Voici un exemple de charge utile d'une notification Amazon SNS qui est générée quand AWS Config détecte que le volume Amazon Elastic Block Store `vol-ce676ccc` est attaché à l'instance dont l'ID est `i-344c463d`. La notification contient la modification apportée à l'élément de configuration pour la ressource.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "accountId": "123456789012",
```

```
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
```

```
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```


Eléments de configuration pour les ressources avec des relations

Si une ressource est liée à d'autres ressources, une modification de celle-ci peut entraîner la création de plusieurs éléments de configuration. L'exemple suivant montre comment AWS Config créer des éléments de configuration pour des ressources ayant des relations.

1. Vous disposez d'une instance Amazon EC2 dont l'ID est `i-007d374c8912e3e90` et qui est associée à un groupe de sécurité Amazon EC2, `sg-c8b141b4`.
2. Vous mettez à jour votre instance EC2 pour remplacer le groupe de sécurité par un autre groupe de sécurité, `sg-3f1fef43`.
3. Comme l'instance EC2 est liée à une autre ressource, elle AWS Config crée plusieurs éléments de configuration, comme dans les exemples suivants :

Cette notification contient la modification apportée à l'élément de configuration pour l'instance EC2 lorsque le groupe de sécurité est remplacé.


```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
```

```
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
```

```
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
```

```
                    "groupId": "sg-c8b141b4"
                },
                "updatedValue": null,
                "changeType": "DELETE"
            }
        },
        "changeType": "UPDATE"
    },
    "configurationItem": {
        "relatedEvents": [],
        "relationships": [
            {
                "resourceId": "eni-fde9493f",
                "resourceName": null,
                "resourceType": "AWS::EC2::NetworkInterface",
                "name": "Contains NetworkInterface"
            },
            {
                "resourceId": "sg-3f1fef43",
                "resourceName": null,
                "resourceType": "AWS::EC2::SecurityGroup",
                "name": "Is associated with SecurityGroup"
            },
            {
                "resourceId": "subnet-2372be7b",
                "resourceName": null,
                "resourceType": "AWS::EC2::Subnet",
                "name": "Is contained in Subnet"
            },
            {
                "resourceId": "vol-0a2d63a256bce35c5",
                "resourceName": null,
                "resourceType": "AWS::EC2::Volume",
                "name": "Is attached to Volume"
            },
            {
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }
        ],
        "configuration": {
            "instanceId": "i-007d374c8912e3e90",
```

```
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
```

```
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
```

```
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
```

```
}
```

Cette notification contient la modification apportée à l'élément de configuration pour le groupe de sécurité EC2, `sg-3f1fef43`, qui est associé à l'instance.


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
```

```
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Comprendre le champ **`configurationItemDiff`** dans les notifications **`ConfigurationItemChangeNotification`** Amazon SNS

AWS Config crée un élément de configuration chaque fois que la configuration d'une ressource change (création/mise à jour/suppression). Pour obtenir la liste des types de ressources pris en charge qui AWS Config peuvent enregistrer, consultezTypes de ressource pris en charge. AWS Config utilise Amazon SNS pour envoyer une notification lorsque les modifications se produisent. La charge utile des notifications Amazon SNS inclut des champs pour vous aider à suivre l'évolution des ressources dans une région donnée. AWS

Pour comprendre pourquoi vous recevez une notification `ConfigurationItemChangeNotification`, consultez les détails `configurationItemDiff`. Les champs varient en fonction du type de modification et peuvent former différentes combinaisons, comme MISE À JOUR-MISE À JOUR, MISE À JOUR-CRÉATION et SUPPRESSION-SUPPRESSION. Vous trouverez ci-dessous des explications sur certaines combinaisons courantes.

MISE À JOUR-CRÉATION et MISE À JOUR-MISE À JOUR

L'exemple suivant inclut les modifications apportées aux relations directes entre les ressources et les configurations des ressources. Les détails `configurationItemDiff` révèlent les informations suivantes :

Action effectuée : Une politique gérée présente dans le compte était associée à un rôle AWS Identity and Access Management (IAM).

Opération de base effectuée : MISE À JOUR (mise à jour du nombre d'associations du type de ressource `AWS::IAM::Policy` dans un compte).

Combinaisons de types de changements :

1. Changement de la relation directe entre les ressources MISE À JOUR-CRÉATION. Un nouvel attachement ou une nouvelle association a été créé(e) entre une politique IAM et un rôle IAM.
2. Changement de la configuration des ressources MISE À JOUR-MISE À JOUR. Le nombre d'associations de politiques IAM est passé de 2 à 3 lorsque la politique était associée au rôle IAM.

Exemple de notification MISE À JOUR-CRÉATION et MISE À JOUR-MISE À JOUR `configurationItemDiff` :

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>>> 1
```

```
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

MISE À JOUR/SUPPRESSION

L'exemple suivant inclut les modifications apportées aux relations directes entre les ressources et les configurations des ressources. Les détails `configurationItemDiff` révèlent les informations suivantes :

Action effectuée : Une politique gérée présente dans le compte était détachée d'un UTILISATEUR IAM.

Opération de base effectuée : MISE À JOUR (mise à jour de la politique d'autorisations associée au type de ressource `AWS::IAM::User`).

Combinaisons de types de modifications : modification de la relation directe entre les ressources MISE À JOUR-SUPPRESSION. L'association entre un utilisateur IAM et une politique IAM dans un compte a été supprimée.

Exemple de notification `configurationItemDiff` MISE À JOUR-SUPPRESSION :

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
```

```
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

SUPPRESSION-SUPPRESSION

L'exemple suivant inclut les modifications apportées aux relations directes entre les ressources et les configurations des ressources. Les détails `configurationItemDiff` révèlent les informations suivantes :

Action effectuée : Un rôle IAM présent dans un compte a été supprimé.

Opération de base exécutée : SUPPRESSION (une ressource du type de ressource `AWS::IAM::Role` a été supprimée).

Combinaisons de types de modifications : modification de la relation directe entre les ressources et modification de la configuration des ressources SUPPRESSION-SUPPRESSION. La suppression du rôle IAM a également supprimé l'association de la politique IAM au rôle IAM.

Exemple de notification `configurationItemDiff` SUPPRESSION-SUPPRESSION :

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
```

```
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

Exemple de notification de diffusion de l'historique de configuration

L'historique de configuration est un ensemble d'éléments de configuration pour un type de ressource sur une période. Voici un exemple de notification envoyée lorsque AWS Config l'historique de configuration d'une ressource CloudTrail de suivi est fourni à votre compte.

```
{
    "Type": "Notification",
```

```
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Exemple de notification de démarrage de la diffusion d'un instantané de configuration

Voici un exemple de notification envoyée par AWS Config quand AWS Config lance la diffusion de l'instantané de configuration pour votre compte.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
```

```
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Exemple de notification de diffusion d'un instantané de configuration

L'instantané de configuration est un ensemble d'éléments de configuration pour toutes les ressources enregistrées et leurs configurations dans votre compte. Voici un exemple de notification envoyée par AWS Config quand un instantané de configuration est diffusé pour votre compte.

```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
```

```
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Exemple de notification de modification de conformité

Quand AWS Config évalue vos ressources par rapport à une règle personnalisée ou gérée, AWS Config envoie une notification qui indique si les ressources sont conformes à la règle.

Voici un exemple de notification dans laquelle la ressource CloudTrail de suivi est conforme à la règle `cloudtrail-enabled` gérée.

```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
```

```
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Exemple : modification de l'élément de configuration de configuration | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
```

```
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
```

```
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

Exemple de notification d'une évaluation de règles démarrée

AWS Config envoie une notification quand il commence à évaluer votre règle personnalisée ou gérée sur vos ressources. Voici un exemple de notification quand AWS Config commence à évaluer la règle gérée `iam-password-policy`.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
```

```
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Exemple de notification de changement avec un élément de configuration trop grand

Quand AWS Config détecte un changement de configuration pour une ressource, il envoie une notification d'élément de configuration. Si la notification dépasse la taille maximale autorisée par Amazon Simple Notification Service (Amazon SNS), elle inclut un bref résumé de l'élément de configuration. Vous pouvez consulter la notification complète dans l'emplacement du compartiment Amazon S3 indiqué dans le `s3BucketLocation` champ.

L'exemple de notification suivant montre un élément de configuration pour une instance Amazon EC2. La notification inclut un résumé des modifications et l'emplacement de la notification dans le compartiment Amazon S3.

```
View the Timeline for this Resource in the Console:
```

```
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/
us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

Exemple de notification d'échec de diffusion

AWS Configenvoie une notification d'échec de livraison si AWS Config vous ne parvenez pas à envoyer l'instantané de configuration ou une notification de modification d'élément de configuration surdimensionné à votre compartiment Amazon S3. Vérifiez que vous avez spécifié un compartiment Amazon S3 valide.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
```

```
    "notificationCreationTime": "2016-10-06T16:46:13.749Z",
    "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
    "recordVersion": "1.0"
  }
```

Gestion et affichage AWS des configurations de ressources avec AWS Config

AWS Config vous permet d'évaluer, d'auditer et d'évaluer les configurations des AWS ressources.

AWS les ressources sont des entités que vous créez et gérez à l' AWS Management Console aide de la AWS Command Line Interface (CLI), AWS des SDK ou des outils AWS partenaires. Les exemples de AWS ressources incluent les instances Amazon EC2, les groupes de sécurité, les Amazon VPC et Amazon Elastic Block Store. AWS Config fait référence à chaque ressource à l'aide de son identifiant unique, tel que l'ID de ressource ou un Amazon Resource Name (ARN).

Certains cas d'utilisation courants incluent :

- Administrateur cloud : vous pouvez suivre et gérer les configurations des ressources pour garantir la conformité, résoudre les problèmes et maintenir une bonne compréhension de votre environnement AWS
- Analyste de sécurité : vous pouvez évaluer les configurations des ressources par rapport aux états souhaités afin d'identifier les vulnérabilités et d'évaluer le niveau de sécurité.
- Responsable de la conformité : vous pouvez auditer et surveiller en permanence les configurations des ressources afin de garantir le respect des politiques organisationnelles et des normes du secteur.

Rubriques

- Afficher le AWS Config tableau de bord
- Types de ressource pris en charge
- Couverture des ressources en fonction de la disponibilité dans les régions
- AWS Ressources d'enregistrement
- Enregistrement de configurations pour les ressources tierces
- Enregistrement de la configuration logicielle pour des instances gérées
- Affichage des configurations de ressource et de l'historique
- Balisage de vos ressources AWS Config

Afficher le AWS Config tableau de bord

Utilisez le tableau de bord pour avoir un aperçu de vos ressources, de vos règles, de vos packs de conformité et de leur état de conformité, ainsi que pour visualiser vos indicateurs AWS Config d'utilisation et de réussite avec Amazon CloudWatch. Cette page vous permet d'identifier rapidement les principales ressources de votre AWS compte, les packs de conformité présentant le plus faible niveau de conformité Compte AWS, les règles ou ressources non conformes dans votre compte Compte AWS, le trafic qui détermine votre AWS Config utilisation et les indicateurs clés de réussite et d'échec de vos flux de travail.

Pour utiliser le AWS Config tableau de bord

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le panneau de navigation de gauche, choisissez Tableau de bord.

Table des matières

- Conformité et inventaire des ressources
- AWS Config Indicateurs d'utilisation et de réussite

Conformité et inventaire des ressources

Après la configuration, AWS Config commence à enregistrer les ressources que vous avez spécifiées et à les évaluer par rapport à vos règles. L'affichage de vos ressources, règles, packs de conformité et de leur état de conformité peut prendre quelques minutes. AWS Config

Packs de conformité en fonction du score de conformité

L'option Packs de conformité en fonction du score de conformité affiche jusqu'à 10 de vos packs de conformité présentant le score de conformité le plus faible. Le score de conformité est le pourcentage du nombre de combinaisons règle-ressource conformes dans un pack de conformité par rapport au nombre total de combinaisons règles-ressources possibles dans le pack de conformité.

Cette métrique vous fournit une vue d'ensemble de l'état de conformité de vos packs de conformité. Elle peut être utilisée pour identifier, étudier et comprendre le niveau de conformité de vos packs de conformité. Vous pouvez utiliser le score de conformité pour suivre la progression

des mesures correctives, effectuer des comparaisons entre différents ensembles d'exigences et évaluer l'impact d'un changement ou d'un déploiement spécifique sur un pack de conformité.

Pour afficher l'état du déploiement, le score de conformité, la chronologie des scores de conformité et les règles d'un pack de conformité dans une vue détaillée, choisissez le nom du pack de conformité dans Pack de conformité.

Statut de conformité

L'État de conformité affiche le nombre de vos règles conformes et non conformes ainsi que le nombre des ressources conformes et non conformes. Les ressources sont conformes ou non conformes d'après l'évaluation de la règle qui leur est associée. Si une ressource ne respecte pas les spécifications de la règle, la ressource et la règle sont signalées comme non conformes.

Pour afficher la liste des règles et ressources non conformes, choisissez Règle(s) non conforme(s) ou Ressource(s) non conforme(s).

Règles en fonction des ressources non conformes

L'option Règles en fonction des ressources non conformes affiche les principales règles non conformes par ordre décroissant en fonction du nombre de ressources. Choisissez une règle pour afficher ses détails, ses paramètres et les ressources concernées par cette règle spécifique.

Pour obtenir une liste complète des règles non conformes, choisissez Afficher toutes les règles non conformes.

Inventaire des ressources

L'inventaire des ressources affiche le nombre total de ressources AWS Config enregistrées par ordre décroissant en fonction du nombre de ressources et du nombre de chaque type de ressource dans votre Compte AWS. Pour ouvrir toutes les ressources d'un type de ressource, choisissez ce type de ressource pour accéder à la page Inventaire des ressources associée.

Vous pouvez utiliser la liste déroulante pour indiquer le total des ressources que vous souhaitez consulter. Par défaut, il est configuré pour afficher toutes les ressources, mais vous pouvez le remplacer par des AWS ressources, des ressources tierces ou des ressources personnalisées.

> **Note**
>
> Le message Évaluez la configuration de vos AWS ressources à l'aide des règles de configuration peut apparaître sur le tableau de bord pour les raisons suivantes :

- Vous n'avez pas défini de AWS Config règles pour votre Compte AWS. Vous pouvez choisir Add rule (Ajouter une règle) pour accéder à la page Rules (Règles).
- AWS Config évalue toujours vos ressources par rapport à vos règles. Vous pouvez actualiser la page pour voir les derniers résultats de l'évaluation.
- AWS Config a évalué vos ressources par rapport à vos règles et n'a trouvé aucune ressource dans le champ d'application. Vous pouvez spécifier les ressources AWS Config à enregistrer dans la page Paramètres. Pour plus d'informations, consultez AWS Ressources d'enregistrement.

AWS Config Indicateurs d'utilisation et de réussite

Vous pouvez utiliser les CloudWatch tableaux de bord Amazon dans la AWS Config console pour visualiser vos indicateurs AWS Config d'utilisation et de réussite.

Vous pouvez procéder comme suit pour chaque tableau de bord :

- Ajustez la plage horaire du tableau de bord pour afficher les données des 3 dernières heures, 1 jour ou 1 semaine.
- Cliquez sur l'icône du calendrier pour saisir un intervalle de temps personnalisé : soit un temps relatif pour une période spécifiée dans le passé, soit un intervalle de temps absolu entre deux dates.
- Vous pouvez modifier le format horaire pour afficher les données du tableau de bord en UTC (temps universel coordonné) ou en fuseau horaire local (le fuseau horaire spécifié comme fuseau horaire local dans le système d'exploitation de votre appareil).
- Utilisez la flèche pointant vers le bas située à côté de l'icône Actualiser pour indiquer la fréquence à laquelle les données d'un tableau de bord doivent être actualisées ou pour désactiver l'actualisation automatique. Choisissez Désactivé, 10 secondes, 1 minute, 2 minutes, 5 minutes ou 15 minutes pour modifier l'actualisation interne.
- Choisissez Plus d'options (le menu à points de suspension verticaux) pour ajouter à la CloudWatch console les indicateurs AWS Config d'utilisation ou les indicateurs de AWS Config succès que vous consultez actuellement dans le AWS Config tableau de bord. Cela ouvre un nouvel onglet dans la CloudWatch console qui vous permet de créer un nouveau tableau de bord personnalisé CloudWatch avec des informations copiées à partir de vos indicateurs AWS Config d'utilisation ou de AWS Config réussite actuels.

Si vous souhaitez effectuer des analyses supplémentaires de ces métriques avec CloudWatch, choisissez Metrics dans le volet de navigation de gauche de la CloudWatch console, puis choisissez AWS/Config. Pour plus d'informations sur ce que vous pouvez faire depuis la CloudWatch console, consultez les sections Utilisation CloudWatch des tableaux de bord Amazon et Utilisation des CloudWatch métriques Amazon dans le guide de l'CloudWatch utilisateur.

AWS Config Métriques d'utilisation

Métrique	Description	Unité	
`Configuration Items Recorded`	Le nombre d'éléments de configuration enregistrés pour chaque type de ressource ou pour tous les types de ressources. Un élément de configuration représente une point-in-time vue des différents attributs d'une AWS ressource prise en charge. Pour plus d'informations sur les éléments de configuration ou les types de ressources pris en charge, consultez Éléments de configuration et Types de ressources pris en charge.	Nombre	

Vous pouvez sélectionner le type de ressource que vous souhaitez consulter à l'aide de la liste déroulante. L'affichage de tous les types de ressources est défini par défaut.

AWS Config Indicateurs de réussite

Métrique	Description	Unité	
`Change Notifications Delivery Failed`	Le nombre de notifications de modification ayant échoué à la rubrique Amazon SNS pour votre canal de diffusion. Une notification de modification vous informe de la modification de l'état de configuration de vos AWS ressources. Vous pouvez utiliser l'ConfigStreamDeliveryInfoAPI pour obtenir `lastErrorCode` ou `lastErrorMessage` pour la dernière tentative de livraison d'une notificat	Nombre	

Métrique	Description	Unité	
	ion de modification. Pour plus d'informations, consultez Gestion du canal de livraison.		
`Config History Export Failed`	Le nombre d'exportations de l'historique de configuration ayant échoué vers votre compartiment Amazon S3. Un historique de configuration est un ensemble d'éléments de configuration pour une ressource donnée sur n'importe quelle période spécifiée. Pour plus d'informations sur l'historique de configura tion, consultez Historique de configuration.	Nombre	
`Configura tion Recorder Insuffici ent Permissio ns Failure`	Le nombre de tentatives d'accès aux autorisat ions infructueuses en raison de la politique de rôle IAM selon laquelle l'enregistreur de configuration ne disposait pas d'autoris ations suffisantes. L'enregistreur de configura tion détecte les changements apportés à vos configurations de ressources et capture ces modifications en tant qu'éléments de configuration. Pour que l'enregistreur de configuration enregistre vos configurations de AWS ressources, il doit disposer des autorisat ions IAM nécessaires. Pour plus d'informa tions, consultez Politique de rôle IAM pour obtenir les détails de configuration.	Nombre	
`Config Snapshot Export Failed`	Le nombre d'exportations de snapshots de configuration échouées vers votre compartim ent Amazon S3. Un instantané de configura tion est un ensemble d'éléments de configura tion pour les ressources prises en charge dans votre compte. Pour plus d'informa tions sur les instantanés de configuration, consultez Instantané de configuration.	Nombre	

Types de ressource pris en charge

> **Important**
>
> Cette page est mise à jour tous les mois au début de chaque mois.

AWS Config prend en charge les types de AWS ressources et les relations de ressources suivants.

- Pour des informations plus détaillées sur un type de ressource, consultez ses informations de référence (telles que la syntaxe, les propriétés et les valeurs de retour) dans la référence aux types de AWS ressources et de propriétés du Guide de l' AWS CloudFormation utilisateur.
- Pour AWS Config l'enregistrement, certaines AWS régions prennent en charge un sous-ensemble de ces types de ressources. Pour en savoir plus sur les types de ressources pris en charge selon les régions, consultez Couverture des ressources en fonction de la disponibilité dans les régions.
- Les requêtes avancées pour les AWS Config supports concernent un sous-ensemble de ces types de ressources. Pour obtenir une liste des types de ressources pris en charge, consultez Types de ressources pris en charge pour les requêtes avancées.
- Évaluation proactive des AWS Config supports pour un sous-ensemble de ces types de ressources. Pour obtenir la liste de ces types de ressources pris en charge, consultez Types pour évaluation proactive.
- Les règles périodiques s'exécutent sans que l'enregistreur de configuration soit activé, car les règles périodiques ne dépendent pas des éléments de configuration. Pour plus d'informations sur la différence entre les règles déclenchées par des modifications et les règles périodiques, voir Mode d'évaluation et types de déclencheurs pour les AWS Config règles.

> **Note**
>
> Avant de spécifier un type de ressource AWS Config à suivre, vérifiez la couverture des ressources par région disponible pour voir si le type de ressource est pris en charge dans la AWS région où vous l'avez configuré AWS Config. Si un type de ressource est pris AWS Config en charge par au moins une région, vous pouvez activer l'enregistrement de ce type de ressource dans toutes les régions prises en charge AWS Config, même si le type de ressource spécifié n'est pas pris en charge dans la AWS région où vous l'avez configuré AWS Config.

Amazon AppStream

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	NA	NA
	`AWS::AppStream::Application`	NA	NA
	`AWS::AppStream::Stack`	NA	NA
	`AWS::AppStream::Fleet`	NA	NA

Amazon AppFlow

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon AppFlow	`AWS::AppFlow::Flow`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	NA	NA

Amazon API Gateway

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
API Gateway	`AWS::ApiGateway::Stage`	est contenu dans	ApiGateway API Rest
		est associé à	WebACL WAFRegional
	`AWS::ApiGateway::RestApi`	contient	ApiGateway Étape
API Gateway V2	`AWS::ApiGatewayV2::Stage`	est contenu dans	ApiGatewayAPI V2
	`AWS::ApiGatewayV2::Api`	contient	ApiGatewayÉtape V2

Pour en savoir plus sur le mode d' AWS Config intégration avec Amazon API Gateway, consultez la section Surveillance de la configuration de l'API API Gateway avec AWS Config.

Amazon Athena

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Athena	`AWS::Athena::WorkGroup`	NA	NA
	`AWS::Athena::DataCatalog`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::Athena::PreparedStatement`	NA	NA

Amazon CloudFront

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon CloudFront	`AWS::CloudFront::Distribution`	est associé à	AWS WebACL WAF
			Certificat ACM
			S3 Bucket
			Certificat de serveur IAM
	`AWS::CloudFront::StreamingDistribution`	est associé à	AWS WebACL WAF
			Certificat ACM
			S3 Bucket
			Certificat de serveur IAM

Amazon CloudWatch

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	NA	NA
	`AWS::CloudWatch::MetricStream`	NA	NA
Amazon CloudWatch Logs	`AWS::Logs::Destination`	NA	NA
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	NA	NA
Amazon, CloudWatch évidemment	`AWS::Evidently::Project`	NA	NA
	`AWS::Evidently::Launch`	NA	NA
	`AWS::Evidently::Segment`	NA	NA

Amazon CodeGuru

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
CodeGuru Réviseur Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	NA	NA

Amazon Cognito

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Cognito	`AWS::Cognito::UserPool`	NA	NA
	`AWS::Cognito::UserPoolClient`	NA	NA
	`AWS::Cognito::UserPoolGroup`	NA	NA

Amazon Connect

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Connect	`AWS::Connect::PhoneNumber`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::Connect::QuickConnect`	NA	NA
	`AWS::Connect::Instance`	NA	NA
Profils des clients Amazon Connect	`AWS::CustomerProfiles::Domain`	NA	NA
	`AWS::CustomerProfiles::ObjectType`	NA	NA

Amazon Detective

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Detective	`AWS::Detective::Graph`	NA	NA

Amazon DynamoDB

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon DynamoDB	`AWS::DynamoDB::Table`	NA	NA

Amazon Elastic Compute Cloud

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	contient	instance EC2
	`AWS::EC2::EIP`	est attaché à	instance EC2
			Interface réseau
	`AWS::EC2::Instance`	contient	Interface réseau EC2
		est associé à	Groupe de sécurité EC2
		est attaché à	Volume Amazon EBS
			EC2 Elastic IP (EIP)
		est contenu dans	Hôte dédié EC2
			Table de routage
			Sous-réseau
			Cloud privé virtuel (VPC)
	`AWS::EC2::NetworkInterface`	est associé à	Groupe de sécurité EC2
		est attaché à	EC2 Elastic IP (EIP)
			instance EC2
		est contenu dans	Table de routage
			Sous-réseau

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
			Cloud privé virtuel (VPC)
	`AWS::EC2::SecurityGroup` *	est associé à	instance EC2
			Interface réseau EC2
			Cloud privé virtuel (VPC)
	`AWS::EC2::NatGateway`	est contenu dans	Virtual Private Cloud (VPC)
		est contenu dans	Sous-réseau
	`AWS::EC2::EgressOnlyInternetGateway`	est attaché à	Cloud privé virtuel (VPC)
	`AWS::EC2::EC2Fleet`	NA	NA
	`AWS::EC2::SpotFleet`	NA	NA
	`AWS::EC2::PrefixList`	NA	NA
	`AWS::EC2::FlowLog`	NA	NA
	`AWS::EC2::TransitGateway`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::EC2::TransitGatewayAttachment`	NA	NA
	`AWS::EC2::TransitGatewayRouteTable`	NA	NA
	`AWS::EC2::VPCEndpoint`	est contenu dans	Virtual Private Cloud (VPC)
		est attaché à	Interface réseau
		est contenu dans	Sous-réseau
		est contenu dans	Table de routage
	`AWS::EC2::VPCEndpointService`	est associé à	ElasticLoadÉquilibrage V2 LoadBalancer
	`AWS::EC2::VPCPeeringConnection`	est associé à	Cloud privé virtuel (VPC)
	`AWS::EC2::RegisteredHAInstance`	est associé à	instance EC2
	`AWS::EC2::SubnetRouteTableAssociation`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::EC2::LaunchTemplate`	NA	NA
	`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	NA	NA
	`AWS::EC2::TrafficMirrorTarget`	NA	NA
	`AWS::EC2::TrafficMirrorSession`	NA	NA
	`AWS::EC2::DHCPOptions`	NA	NA
	`AWS::EC2::IPAM`	NA	NA
	`AWS::EC2::NetworkInsightsPath`	NA	NA
	`AWS::EC2::TrafficMirrorFilter`	NA	NA
	`AWS::EC2::CapacityReservation`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::EC2::ClientVpnEndpoint`	NA	NA
	`AWS::EC2::CustomerGateway`	est attaché à	Connexion VPN
	`AWS::EC2::InternetGateway`	est attaché à	Cloud privé virtuel (VPC)
	`AWS::EC2::NetworkAcl`	NA	NA
	`AWS::EC2::RouteTable`	contient	instance EC2
			Interface réseau EC2
			Sous-réseau
			Passerelle VPN
		est contenu dans	Virtual Private Cloud (VPC)
	`AWS::EC2::Subnet`	contient	instance EC2
			Interface réseau EC2
		est attaché à	ACL réseau
		est contenu dans	Table de routage
			Cloud privé virtuel (VPC)

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::EC2::VPC`	contient	instance EC2
			Interface réseau EC2
			Réseau ACL
			Table de routage
			Sous-réseau
		est associé à	Groupe de sécurité
		est attaché à	Passerelle Internet
			Passerelle VPN
	`AWS::EC2::VPNConnection`	est attaché à	Passerelle client
			Passerelle VPN
	`AWS::EC2::VPNGateway`	est attaché à	Cloud privé virtuel (VPC)
			Connexion VPN
		est contenu dans	Table de routage
	`AWS::EC2::IPAMScope`	NA	NA
	`AWS::EC2::CarrierGateway`	NA	NA
	`AWS::EC2::TransitGatewayConnect`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::EC2::IPAMPool`	NA	NA
	`AWS::EC2::TransitGatewayMulticastDomain`	NA	NA
	`AWS::EC2::NetworkInsightsAccessScope`	NA	NA
	`AWS::EC2::NetworkInsightsAnalysis`	NA	NA
Amazon Elastic Block Store	`AWS::EC2::Volume`	est attaché à	instance EC2
EC2 Image Builder	`AWS::ImageBuilder::ImagePipeline`	NA	NA
	`AWS::ImageBuilder::DistributionConfiguration`	NA	NA
	`AWS::ImageBuilder::ContainerRecipe`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::ImageBuilder::InfrastructureConfiguration`	NA	NA
	`AWS::ImageBuilder::ImageRecipe`	NA	NA

*AWS Config enregistre les détails de configuration des hôtes dédiés et des instances que vous y lancez. Par conséquent, vous pouvez l'utiliser AWS Config comme source de données lorsque vous signalez la conformité à vos licences logicielles liées au serveur. Par exemple, vous pouvez afficher l'historique de configuration d'une instance et déterminer l'Amazon Machine Image (AMI) sur laquelle il repose. Ensuite, vous pouvez rechercher l'historique de configuration de l'hôte, qui inclut des détails comme les nombres de sockets et de cœurs, pour vérifier que l'hôte respecte les exigences de licence de l'image AMI. Pour plus d'informations, consultez la section Suivi des modifications de configuration AWS Config dans le guide de l'utilisateur Amazon EC2.

* La définition des SecurityGroup propriétés EC2 contient des blocs d'adresse IP CIDR, qui sont convertis en plages d'adresses IP en interne, et peuvent renvoyer des résultats inattendus lorsque vous essayez de trouver une plage d'adresses IP spécifique. Pour trouver des solutions permettant de rechercher des plages d'adresses IP spécifiques, consultez Limitations relatives aux requêtes avancées.

Amazon Elastic Container Registry

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Elastic Container Registry	`AWS::ECR::Repository`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::ECR::Registry Policy`	NA	NA
	`AWS::ECR::PullThroughCacheRule`	NA	NA
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	NA	NA

Amazon Elastic Container Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Elastic Container Service	`AWS::ECS::Cluster`	NA	NA
	`AWS::ECS::TaskDefinition`	NA	NA
	`AWS::ECS::Service` *	NA	NA
	`AWS::ECS::TaskSet`	NA	NA
	`AWS::ECS::CapacityProvider`	NA	NA

*Ce service ne prend actuellement en charge que le nouveau format Amazon Resource Name (ARN). Pour plus d'informations, consultez Amazon Resource Names (ARN) et ID dans le Guide du développeur ECS.

Ancien (non pris en charge) : `arn:aws:ecs:region:aws_account_id:service/service-name`

Nouveau (pris en charge) : `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Amazon Elastic File System

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Elastic File System	`AWS::EFS::FileSystem`	NA	NA
	`AWS::EFS::AccessPoint`	NA	NA

Amazon Elastic Kubernetes Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	NA	NA
	`AWS::EKS::FargateProfile`	NA	NA
	`AWS::EKS::IdentityProviderConfig`	NA	NA
	`AWS::EKS::Addon`	NA	NA

Amazon EMR

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon EMR	`AWS::EMR::Security Configuration`	NA	NA

Amazon EventBridge

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon EventBridge	`AWS::Events::EventBus`	NA	NA
	`AWS::Events::ApiDestination`	NA	NA
	`AWS::Events::Archive`	NA	NA
	`AWS::Events::Endpoint`	NA	NA
	`AWS::Events::Connection`	NA	NA
	`AWS::Events::Rule`	NA	NA
EventBridge Schémas Amazon	`AWS::EventSchemas::Registry Policy`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::EventSchemas::Discoverer`	NA	NA
	`AWS::EventSchemas::Schema`	NA	NA

Amazon Forecast

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Forecast	`AWS::Forecast::Dataset`	NA	NA
	`AWS::Forecast::DatasetGroup`	NA	NA

Amazon Fraud Detector

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Fraud Detector	`AWS::FraudDetector::Label`	NA	NA
	`AWS::FraudDetector::EntityType`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::FraudDetector::Variable`	NA	NA
	`AWS::FraudDetector::Outcome`	NA	NA

Amazon GuardDuty

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon GuardDuty	`AWS::GuardDuty::Detector`	NA	NA
	`AWS::GuardDuty::ThreatIntelSet`	NA	NA
	`AWS::GuardDuty::IPSet`	NA	NA
	`AWS::GuardDuty::Filter`	NA	NA

Amazon Inspector

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Inspector	`AWS::InspectorV2::Filter`	NA	NA

Amazon Interactive Video Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Interactive Video Service	`AWS::IVS::Channel`	NA	NA
	`AWS::IVS::RecordingConfiguration`	NA	NA
	`AWS::IVS::PlaybackKeyPair`	NA	NA

Amazon Keyspaces (pour Apache Cassandra)

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Keyspaces (pour Apache Cassandra)	`AWS::Cassandra::Keyspace`	NA	NA

Amazon OpenSearch Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon OpenSearch Service	`AWS::Elasticsearch::Domain`	est associé à	Clé KMS
			Groupe de sécurité EC2
			Sous-réseau EC2
			Cloud privé virtuel (VPC)
	`AWS::OpenSearch::Domain`	NA	NA

> **Note**
>
> Le 8 septembre 2021, Amazon Elasticsearch Service a été renommé Amazon Service. OpenSearch OpenSearch Le service prend en charge OpenSearch ainsi que l'ancien logiciel Elasticsearch OSS. Pour plus d'informations, consultez Amazon OpenSearch Service - Résumé des modifications.
> Vous pouvez continuer à consulter vos données `AWS::OpenSearch::Domain` sous le type de `AWS::Elasticsearch::Domain` ressource existant pendant plusieurs semaines, même si vous effectuez la mise à niveau d'un ou de plusieurs domaines vers OpenSearch.

Amazon Personalize

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Personalize	`AWS::Personalize::Dataset`	NA	NA
	`AWS::Personalize::Schema`	NA	NA
	`AWS::Personalize::Solution`	NA	NA
	`AWS::Personalize::DatasetGroup`	NA	NA

Amazon Pinpoint

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	NA	NA
	`AWS::Pinpoint::Segment`	NA	NA
	`AWS::Pinpoint::App`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::Pinpoint::Campaign`	NA	NA
	`AWS::Pinpoint::InAppTemplate`	NA	NA
	`AWS::Pinpoint::EmailChannel`	NA	NA
	`AWS::Pinpoint::EmailTemplate`	NA	NA
	`AWS::Pinpoint::EventStream`	NA	NA

Amazon Quantum Ledger Database (Amazon QLDB)

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon QLDB	`AWS::QLDB::Ledger`	NA	NA

Amazon Kendra

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Kendra	`AWS::Kendra::Index`	NA	NA

Amazon Kinesis

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Kinesis	`AWS::Kinesis::Stream`	NA	NA
	`AWS::Kinesis::StreamConsumer`	NA	NA
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	NA	NA
Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`	NA	NA
Flux vidéo Kinesis	`AWS::KinesisVideo::SignalingChannel`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::KinesisVideo::Stream`	NA	NA

Amazon Lex

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Lex	`AWS::Lex::BotAlias`	NA	NA
	`AWS::Lex::Bot`	NA	NA

Amazon Lightsail

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Lightsail	`AWS::Lightsail::Disk`	NA	NA
	`AWS::Lightsail::Certificate`	NA	NA
	`AWS::Lightsail::Bucket`	NA	NA
	`AWS::Lightsail::StaticIp`	NA	NA

Amazon Lookout for Metrics

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Lookout for Metrics	`AWS::LookoutMetrics::Alert`	NA	NA

Amazon Lookout for Vision

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	NA	NA

Amazon Managed Grafana

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Managed Grafana	`AWS::Grafana::Workspace`	NA	NA

Amazon Managed Service for Prometheus

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Managed Service for Prometheus	`AWS::APS::RuleGroupsNamespace`	NA	NA

Amazon MemoryDB for Redis

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon MemoryDB for Redis	`AWS::MemoryDB::SubnetGroup`	NA	NA

Amazon MQ

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon MQ	`AWS::AmazonMQ::Broker`	NA	NA

Amazon Managed Streaming for Apache Kafka

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Managed Streaming for Apache Kafka	`AWS::MSK::Cluster`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::MSK::Configuration`	NA	NA
	`AWS::MSK::BatchScramSecret`	NA	NA
	`AWS::MSK::ClusterPolicy`	NA	NA
	`AWS::MSK::VpcConnection`	NA	NA
Amazon Managed Streaming pour Apache Kafka	`AWS::KafkaConnect::Connector`	NA	NA

Amazon Redshift

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Redshift	`AWS::Redshift::Cluster`	est associé à	Groupe de paramètres du cluster
			Groupe de sécurité du cluster
			Groupe de sous-réseaux du cluster
			Groupe de sécurité
			Cloud privé virtuel (VPC)

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::Redshift::ClusterParameterGroup`	NA	NA
	`AWS::Redshift::ClusterSecurityGroup`	NA	NA
	`AWS::Redshift::ScheduledAction`	NA	NA
	`AWS::Redshift::ClusterSnapshot`	est associé à	Cluster
			Cloud privé virtuel (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	est associé à	Sous-réseau
			Cloud privé virtuel (VPC)
	`AWS::Redshift::EventSubscription`	NA	NA
	`AWS::Redshift::EndpointAccess`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::Redshift::EndpointAuthorization`	NA	NA

Amazon Relational Database Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Relational Database Service	`AWS::RDS::DBInstance`	est associé à	Groupe de sécurité EC2
			Security group DB RDS
			Groupe de sous-rése aux DB RDS
	`AWS::RDS::DBSecurityGroup`	est associé à	Groupe de sécurité EC2
			Cloud privé virtuel (VPC)
	`AWS::RDS::DBSnapshot`	est associé à	Cloud privé virtuel (VPC)
	`AWS::RDS::DBSubnetGroup`	est associé à	Groupe de sécurité EC2
			Cloud privé virtuel (VPC)

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::RDS::EventSubscription`	NA	NA
	`AWS::RDS::DBCluster`	contient	Instance DB RDS
		est associé à	Groupe de sous-réseaux DB RDS
			Groupe de sécurité EC2
	`AWS::RDS::DBClusterSnapshot`	est associé à	Cluster de base de données RDS
			Cloud privé virtuel (VPC)
	`AWS::RDS::GlobalCluster`	NA	NA
	`AWS::RDS::OptionGroup`	NA	NA

Amazon Route 53

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Route 53	`AWS::Route53::HostedZone`	NA	NA
	`AWS::Route53::HealthCheck`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Route 53 Resolver	AWS::Route53Resolver::ResolverEndpoint	NA	NA
	AWS::Route53Resolver::ResolverRule	NA	NA
	AWS::Route53Resolver::ResolverRuleAssociation	NA	NA
	AWS::Route53Resolver::FirewallDomainList	NA	NA
	AWS::Route53Resolver::FirewallRuleGroupAssociation	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfig	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	NA	NA
	AWS::Route53Resolver::FirewallRuleGroup	NA	NA
Application Recovery Controller Amazon Route 53	AWS::Route53RecoveryReadiness::Cell	NA	NA
	AWS::Route53RecoveryReadiness::ReadinessCheck	NA	NA
	AWS::Route53RecoveryReadiness::RecoveryGroup	NA	NA
	AWS::Route53RecoveryControl::Cluster	NA	NA
	AWS::Route53RecoveryControl::ControlPanel	NA	NA
	AWS::Route53RecoveryControl::RoutingControl	NA	NA
	AWS::Route53RecoveryControl::SafetyRule	NA	NA
	AWS::Route53RecoveryReadiness::ResourceSet	NA	NA

Amazon SageMaker

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon SageMaker	`AWS::SageMaker::CodeRepository`	NA	NA
	`AWS::SageMaker::Domain`	NA	NA
	`AWS::SageMaker::AppImageConfig`	NA	NA
	`AWS::SageMaker::Image`	NA	NA
	`AWS::SageMaker::Model`	NA	NA
	`AWS::SageMaker::NotebookInstance`	NA	NA
	`AWS::SageMaker::NotebookInstanceLifecycleConfig`	NA	NA
	`AWS::SageMaker::EndpointConfig`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::SageMaker::Workteam`	NA	NA
	`AWS::SageMaker::FeatureGroup`	NA	NA

Amazon Simple Email Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Simple Email Service	`AWS::SES::ConfigurationSet`	NA	NA
	`AWS::SES::ContactList`	NA	NA
	`AWS::SES::Template`	NA	NA
	`AWS::SES::ReceiptFilter`	NA	NA
	`AWS::SES::ReceiptRuleSet`	NA	NA

Amazon Simple Notification Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Simple Notification Service	`AWS::SNS::Topic`	NA	NA

Amazon Simple Queue Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Simple Queue Service	`AWS::SQS::Queue`	NA	NA

Amazon Simple Storage Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon Simple Storage Service	`AWS::S3::Bucket` *	NA	NA
	`AWS::S3::AccountPublicAccessBlock`	NA	NA
	`AWS::S3::MultiRegionAccessPoint`	NA	NA
	`AWS::S3::StorageLens`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::S3::AccessPoint`	NA	NA

* Si vous avez configuré AWS Config pour enregistrer vos compartiments S3 et que vous ne recevez pas de notifications de modification de configuration, vérifiez que vos politiques de compartiment S3 disposent des autorisations requises. Pour plus d'informations, consultez Gestion des autorisations pour l'enregistrement du compartiment S3.

Attributs du compartiment Amazon S3

AWS Config enregistre également les attributs suivants pour le type de ressource du compartiment Amazon S3.

Attributs	Description
AccelerateConfiguration	Accélération du transfert pour les données sur de longues distances entre le client et un compartiment.
BucketAcl	Listes de contrôle d'accès utilisées pour accéder aux compartiments et objets.
BucketPolicy	Stratégie qui définit les autorisations pour le compartiment.
CrossOriginConfiguration	Autoriser les demandes cross-origine vers le compartiment.
LifecycleConfiguration	Règles qui définissent le cycle de vie des objets de votre compartiment.
LoggingConfiguration	Journalisation utilisée pour suivre les demandes d'accès au compartiment.
NotificationConfiguration	Notifications d'événement utilisées pour envoyer des alertes ou déclencher des flux de travail pour des événements de compartiment spécifiés.

Attributs	Description
ReplicationConfiguration	Copie asynchrone automatique d'objets entre des compartiments de différentes régions AWS .
RequestPaymentConfiguration	Le paiement par le demandeur est activé.
TaggingConfiguration	Balises ajoutées au compartiment pour classer par catégorie . Vous pouvez également utiliser le balisage pour suivre la facturation.
WebsiteConfiguration	L'hébergement du site web statique est activé pour le compartiment.
VersioningConfiguration	La gestion des versions est activée pour les objets du compartiment.

Pour plus d'informations sur les attributs, consultez Options de configuration des compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

Amazon WorkSpaces

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	NA	NA
	`AWS::WorkSpaces::Workspace`	NA	NA

AWS Amplify

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Amplify	`AWS::Amplify::App`	NA	NA
	`AWS::Amplify::Branch`	NA	NA

AWS AppConfig

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS AppConfig	`AWS::AppConfig::Application`	NA	NA
	`AWS::AppConfig::Environment`	NA	NA
	`AWS::AppConfig::ConfigurationProfile`	NA	NA
	`AWS::AppConfig::DeploymentStrategy`	NA	NA
	`AWS::AppConfig::HostedConfi`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`gurationVersion`		
	`AWS::AppConfig::ExtensionAssociation`	NA	NA

AWS App Runner

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS App Runner	`AWS::AppRunner::VpcConnector`	NA	NA
	`AWS::AppRunner::Service`	NA	NA

AWS App Mesh

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS App Mesh	`AWS::AppMesh::VirtualNode`	NA	NA
	`AWS::AppMesh::VirtualService`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::AppMesh::VirtualGateway`	NA	NA
	`AWS::AppMesh::VirtualRouter`	NA	NA
	`AWS::AppMesh::Route`	NA	NA
	`AWS::AppMesh::GatewayRoute`	NA	NA
	`AWS::AppMesh::Mesh`	NA	NA

AWS AppSync

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS AppSync	`AWS::AppSync::GraphQLApi`	NA	NA

AWS Audit Manager

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Audit Manager	`AWS::AuditManager::Assessment`	NA	NA

AWS Auto Scaling

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contient	Instance Amazon EC2
		est associé à	Classic Load Balancer
			Configuration de lancement d'Auto Scaling
			Sous-réseau
	`AWS::AutoScaling::LaunchConfiguration`	est associé à	Groupe de sécurité Amazon EC2
	`AWS::AutoScaling::ScalingPolicy`	est associé à	Groupe Auto Scaling
			alerte
	`AWS::AutoScaling::ScheduledAction`	est associé à	Groupe Auto Scaling

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::AutoScaling::WarmPool`	NA	NA

AWS Backup

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Backup	`AWS::Backup::BackupPlan`	NA	NA*
	`AWS::Backup::BackupSelection`	NA	NA
	`AWS::Backup::BackupVault`	NA	NA*
	`AWS::Backup::RecoveryPoint`	NA	NA
	`AWS::Backup::ReportPlan`	NA	NA

En raison du mode de AWS Backup fonctionnement, certains de ces types de ressources sont liés aux autres types de AWS Backup ressources de ce tableau.

`AWS::Backup::BackupPlan`est lié à l'`AWS::Backup::BackupSelection`endroit où un plan de sauvegarde comporte de nombreuses sélections, et `AWS::Backup::BackupVault` à

l'`AWS::Backup::RecoveryPoint`endroit où un AWS Backup coffre-fort possède plusieurs points de restauration.

Pour plus d'informations, consultez Gestion des sauvegardes à l'aide de plans de sauvegarde et Utiliser des coffres de sauvegarde.

AWS Batch

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Batch	`AWS::Batch::JobQueue`	NA	NA
	`AWS::Batch::ComputeEnvironment`	NA	NA
	`AWS::Batch::SchedulingPolicy`	NA	NA

AWS Budgets

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Budgets	`AWS::Budgets::BudgetsAction`	NA	NA

AWS Certificate Manager

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Certificate Manager	`AWS::ACM::Certificate`	NA	NA

AWS CloudFormation

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS CloudFormation	`AWS::CloudFormation::Stack` *	contient	Types de AWS ressources pris en charge

*AWS Config enregistre les modifications de configuration apportées aux AWS CloudFormation piles et aux types de ressources pris en charge dans les piles. AWS Config n'enregistre pas les modifications de configuration pour les types de ressources de la pile qui ne sont pas encore pris en charge. Les types de ressources non pris en charge apparaissent dans la section de configuration supplémentaire de l'élément de configuration de la pile.

AWS CloudTrail

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS CloudTrail	`AWS::CloudTrail::Trail`	NA	NA

AWS Cloud9

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	NA	NA

AWS Cloud Map

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Découverte de service	`AWS::ServiceDiscovery::Service`	NA	NA
	`AWS::ServiceDiscovery::PublicDnsNamespace`	NA	NA
	`AWS::ServiceDiscovery::HttpNamespace`	NA	NA
`AWS::ServiceDiscovery::Instance`	NA	NA	

AWS CodeArtifact

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	NA	NA

AWS CodeBuild

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS CodeBuild	`AWS::CodeBuild::Project` *	est associé à	Compartiment S3
			Rôle IAM
	`AWS::CodeBuild::ReportGroup`	NA	NA

* Pour en savoir plus sur le mode d' AWS Config intégration avec Sample AWS CodeBuild, voir Utiliser AWS Config avec AWS CodeBuild Sample.

AWS CodeDeploy

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS CodeDeploy	`AWS::CodeDeploy::Application`	contient	DeploymentGroup
	`AWS::CodeDeploy::D`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`eployment Config`		
	`AWS::Code Deploy::D eploymentGroup`	est contenu dans	Application

AWS CodePipeline

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS CodePipeline	`AWS::Code Pipeline: :Pipeline` *	est attaché à	Compartiment S3
		est associé à	Rôle IAM
			Projet de code
			Fonction Lambda
			Pile CloudFormation
			ElasticBeanstalk candidature

*AWS Config enregistre les modifications de configuration apportées aux CodePipeline pipelines et aux types de ressources pris en charge dans les pipelines. AWS Config n'enregistre pas les modifications de configuration pour les types de ressources dans les pipelines qui ne sont pas encore pris en charge. Les types de ressource non pris en charge comme `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, et `ECS service` figurent dans la section de configuration supplémentaire de l'élément de configuration de la pile.

AWS Config

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Config	`AWS::Config::ResourceCompliance` *	est associé à	Toutes les ressources *
	`AWS::Config::ConformancePackCompliance`	NA	NA
	`AWS::Config::ConfigurationRecorder` *	NA	NA

*La relation entre une ressource `AWS::Config::ResourceCompliance` et une ressource connexe dépend de la façon dont `AWS::Config::ResourceCompliance` établit les rapports de conformité pour ce type de ressource spécifique.

* `AWS::Config::ConfigurationRecorder` est un type de ressource système AWS Config et l'enregistrement de ce type de ressource est activé par défaut.

> **Note**
>
> L'enregistrement pour les types de ressources `AWS::Config::ConformancePackCompliance` et `AWS::Config::ConfigurationRecorder` est gratuit.

AWS Database Migration Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Database Migration Service	`AWS::DMS::EventSubscription`	NA	NA
	`AWS::DMS::ReplicationSubnetGroup`	NA	NA
	`AWS::DMS::ReplicationInstance`	NA	NA
	`AWS::DMS::ReplicationTask`	NA	NA
	`AWS::DMS::Certificate`	NA	NA
	`AWS::DMS::Endpoint`	NA	NA

AWS DataSync

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS DataSync	`AWS::DataSync::LocationSMB`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::DataSync::LocationFSxLustre`	NA	NA
	`AWS::DataSync::LocationFSxWindows`	NA	NA
	`AWS::DataSync::LocationS3`	NA	NA
	`AWS::DataSync::LocationEFS`	NA	NA
	`AWS::DataSync::LocationNFS`	NA	NA
	`AWS::DataSync::LocationHDFS`	NA	NA
	`AWS::DataSync::LocationObjectStorage`	NA	NA
	`AWS::DataSync::Task`	NA	NA

AWS Device Farm

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	NA	NA
	`AWS::DeviceFarm::InstanceProfile`	NA	NA
	`AWS::DeviceFarm::Project`	NA	NA

AWS Elastic Beanstalk

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	contient	Version de l'application Elastic Beanstalk
			Environnement Elastic Beanstalk
		est associé à	Rôle IAM
	`AWS::ElasticBeanstalk::ApplicationVersion`	est contenu dans	Applications Elastic Beanstalk
		est associé à	Environnement Elastic Beanstalk
			Compartiment S3

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::ElasticBeanstalk::Environment`	est contenu dans	Applications Elastic Beanstalk
		est associé à	Version de l'application Elastic Beanstalk
			Rôle IAM
		contient	CloudFormation Empilez

AWS Fault Injection Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	NA	NA

AWS Global Accelerator

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	NA	NA
	`AWS::GlobalAccelerator::EndpointGroup`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::GlobalAccelerator::Accelerator`	NA	NA

AWS Glue

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Glue	`AWS::Glue::Job`	NA	NA
	`AWS::Glue::Classifier`	NA	NA
	`AWS::Glue::MLTransform`	NA	NA

AWS Ground Station

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Ground Station	`AWS::GroundStation::Config`	NA	NA
	`AWS::GroundStation::MissionProfile`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::GroundStation::DataflowEndpointGroup`	NA	NA

AWS HealthLake

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	NA	NA

AWS Identity and Access Management (JE SUIS)

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Identity and Access Management	`AWS::IAM::User`	est attaché à	Groupe IAM
			Stratégie IAM gérée par le client
	`AWS::IAM::Group`	contient	Utilisateur IAM
		est attaché à	Stratégie IAM gérée par le client
	`AWS::IAM::Role`	est attaché à	Stratégie IAM gérée par le client

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::IAM::Policy`	est attaché à	Utilisateur IAM
			Groupe IAM
			Rôle IAM
	`AWS::IAM::SAMLProvider`	NA	NA
	`AWS::IAM::ServerCertificate`	NA	NA
	`AWS::IAM::InstanceProfile`	NA	NA
	`AWS::IAM::OIDCProvider`	NA	NA
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	NA	NA

AWS Config inclut des politiques intégrées avec les détails de configuration qu'il enregistre. Pour de plus amples informations sur les politiques en ligne, consultez Politiques gérées et politiques en ligne dans le Guide de l'utilisateur IAM.

AWS IoT

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS IoT	`AWS::IoT::Authorizer`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::IoT::Security Profile`	NA	NA
	`AWS::IoT::RoleAlias`	NA	NA
	`AWS::IoT::Dimension`	NA	NA
	`AWS::IoT::Policy`	NA	NA
	`AWS::IoT::MitigationAction`	NA	NA
	`AWS::IoT::ScheduledAudit`	NA	NA
	`AWS::IoT::AccountAuditConfiguration`	NA	NA
	`AWS::IoTSiteWise::Gateway`	NA	NA
	`AWS::IoT::CustomMetric`	NA	NA
	`AWS::IoT::JobTemplate`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::IoT::ProvisioningTemplate`	NA	NA
	`AWS::IoT::CACertificate`	NA	NA
AWS IoT Wireless	`AWS::IoTWireless::ServiceProfile`	NA	NA
	`AWS::IoTWireless::MulticastGroup`	NA	NA
	`AWS::IoTWireless::FuotaTask`	NA	NA
AWS IoT Core	`AWS::IoT::FleetMetric`	NA	NA
AWS IoT Analytics	`AWS::IoTAnalytics::Datastore`	NA	NA
	`AWS::IoTAnalytics::Dataset`	NA	NA
	`AWS::IoTAnalytics::Pipeline`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::IoTAnalytics::Channel`	NA	NA
AWS IoT Events	`AWS::IoTEvents::Input`	NA	NA
	`AWS::IoTEvents::DetectorModel`	NA	NA
	`AWS::IoTEvents::AlarmModel`	NA	NA
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`	NA	NA
	`AWS::IoTTwinMaker::Entity`	NA	NA
	`AWS::IoTTwinMaker::Scene`	NA	NA
	`AWS::IoTTwinMaker::SyncJob`	NA	NA
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::IoTSiteWise::Project`	NA	NA
	`AWS::IoTSiteWise::Portal`	NA	NA
	`AWS::IoTSiteWise::AssetModel`	NA	NA
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	NA	NA

AWS Key Management Service

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Key Management Service	`AWS::KMS::Key`	NA	NA
	`AWS::KMS::Alias`	NA	NA

AWS Lambda

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Lambda	`AWS::Lambda::Function`	est associé à	Rôle IAM

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
			Groupe de sécurité EC2
		est contenu dans	Sous-réseau EC2
	`AWS::Lambda::Alias`	NA	NA
	`AWS::Lambda::CodeSigningConfig`	NA	NA

AWS Mainframe Modernization

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Mainframe Modernization	`AWS::M2::Environment`	NA	NA

AWS Network Firewall

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	est attaché à	Sous-réseau EC2
		est associé à	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewa`	est associé à	NetworkFirewall RuleGroup

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`ll::Firewallpolicy`		
	`AWS::NetworkFirewall::RuleGroup`	NA	NA
	`AWS::NetworkFirewall::TLSInspectionConfiguration`	NA	NA

AWS Network Manager

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	NA	NA
	`AWS::NetworkManager::Site`	NA	NA
	`AWS::NetworkManager::Device`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::NetworkManager::Link`	NA	NA
	`AWS::NetworkManager::GlobalNetwork`	NA	NA
	`AWS::NetworkManager::CustomerGatewayAssociation`	NA	NA
	`AWS::NetworkManager::LinkAssociation`	NA	NA
	`AWS::NetworkManager::ConnectPeer`	NA	NA

AWS Panorama

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Panorama	`AWS::Panorama::Package`	NA	NA

AWS Private Certificate Authority

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	NA	NA
	`AWS::ACMPCA::CertificateAuthorityActivation`	NA	NA

AWS Resilience Hub

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	NA	NA
	`AWS::ResilienceHub::App`	NA	NA

Explorateur de ressources AWS

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Explorateur de ressources AWS	`AWS::ResourceExplorer2::Index`	NA	NA

AWS RoboMaker

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	NA	NA
	`AWS::RoboMaker::RobotApplication`	NA	NA
	`AWS::RoboMaker::SimulationApplication`	NA	NA

AWS Signer

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Signer	`AWS::Signer::SigningProfile`	NA	NA

AWS Secrets Manager

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Secrets Manager	`AWS::SecretsManager::Secret`	est associé à	Fonction Lambda
		est associé à	Clé KMS

AWS Service Catalog

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	est contenu dans	Portefeuille
		est associé à	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	est associé à	Portefeuille
			CloudFormationProduit

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
			CloudFormationEmpilez
	`AWS::ServiceCatalog::Portfolio`	contient	CloudFormationProduit

AWS Shield

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Shield	`AWS::Shield::Protection`	est associé à	CloudFront Distribution sur Amazon
	`AWS::ShieldRegional::Protection`	est associé à	EC2 EIP
		est associé à	ElasticLoadBalancing Équilibreur
		est associé à	ElasticLoadÉquilibrage V2 LoadBalancer

AWS Step Functions

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Step Functions	`AWS::StepFunctions::Activity`	NA	NA

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
	`AWS::StepFunctions::StateMachine`	NA	NA

AWS Systems Manager

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Systems Manager	`AWS::SSM::ManagedInstanceInventory` *	est associé à	instance EC2
	`AWS::SSM::PatchCompliance`	est associé à	Inventaire des instances gérées
	`AWS::SSM::AssociationCompliance`	est associé à	Inventaire des instances gérées
	`AWS::SSM::FileData`	est associé à	Inventaire des instances gérées
	`AWS::SSM::Document`	NA	NA

*Pour en savoir plus sur l'inventaire des instances gérées, consultez Recording Software Configuration for Managed Instances.

AWS Transfer Family

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Transfer Family	`AWS::Transfer::Agreement`	NA	NA
	`AWS::Transfer::Connector`	NA	NA
	`AWS::Transfer::Workflow`	NA	NA
	`AWS::Transfer::Certificate`	NA	NA
	`AWS::Transfer::Profile`	NA	NA

AWS WAF

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS WAF	`AWS::WAF::RateBasedRule`	NA	NA
	`AWS::WAF::Rule`	NA	NA
	`AWS::WAF::WebACL`	est associé à	Règle WAF
			Règle basée sur le débit WAF

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
			Groupe de règles WAF
	`AWS::WAF::RuleGroup`	est associé à	Règle WAF
	`AWS::WAFRegional::RateBasedRule`	NA	NA
	`AWS::WAFRegional::Rule`	NA	NA
	`AWS::WAFRegional::WebACL`	est associé à	ElasticLoadÉquilibrage V2 LoadBalancer
			Règle WAFRegional
			Règle basée sur le débit WAFRegional
			Groupe de règles WAFRegional
	`AWS::WAFRegional::RuleGroup`	est associé à	Règle WAFRegional
AWS WAF V2	`AWS::WAFv2::WebACL`	est associé à	ElasticLoadÉquilibrage V2 LoadBalancer
			ApiGateway Étape
			IPSet WAFv2
			WAF V2 RegexPatternSet

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
			WAF V2 RuleGroup
			WAF V2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	est associé à	IPSet WAFv2
			WAF V2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	est associé à	WAF V2 RuleGroup
	`AWS::WAFv2::IPSet`	NA	NA
	`AWS::WAFv2::RegexPatternSet`	NA	NA

AWS X-Ray

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS X-Ray	`AWS::XRay::EncryptionConfig`	NA	NA

Elastic Load Balancing

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
Elastic Load Balancing	Application Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	est associé à	Groupe de sécurité EC2
		est attaché à	Sous-réseau
		est contenu dans	Virtual Private Cloud (VPC)
	Écouteur Application Load Balancer `AWS::ElasticLoadBalancingV2::Listener`	NA	NA
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	est associé à	Groupe de sécurité EC2
		est attaché à	Sous-réseau
		est contenu dans	Virtual Private Cloud (VPC)
	Network Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	NA	NA

AWS Elemental MediaConnect

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	NA	NA
	`AWS::MediaConnect::FlowVpcInterface`	NA	NA
	`AWS::MediaConnect::FlowSource`	NA	NA

AWS Elemental MediaPackage

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	NA	NA
	`AWS::MediaPackage::PackagingConfiguration`	NA	NA

AWS Elemental MediaTailor

AWS Service	Valeur de type de ressource	Relation	Ressource connexe
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	NA	NA

Couverture des ressources en fonction de la disponibilité dans les régions

Régions Amérique du Nord et du Sud

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::ACM::Certificate	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ACMPCA::CertificateAuthority	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ACMPCA::CertificateAuthorityActivation	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::APS::RuleGroupsEspace de noms	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::AccessAnalyzer::Analyzer	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AmazonMQ::Broker	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Amplify::App	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Amplify::Branch	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ApiGateway::RestApi	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ApiGateway::Stage	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::ApiGatewayV2::Api	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ApiGatewayV2::Stage	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppConfig::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppConfig::ConfigurationProfile	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppConfig::DeploymentStrategy	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppConfig::Environment	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppConfig::ExtensionAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::AppConfig::HostedConfigurationVersion	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppFlow::Flow	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppIntegrations::EventIntegration	Non	Non	Oui	Oui	Non	Oui	Non
AWS::AppMesh::GatewayRoute	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppMesh::Mesh	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppMesh::Route	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppMesh::VirtualGateway	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::AppMesh::VirtualNode	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppMesh::VirtualRouter	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppMesh::VirtualService	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AppRunner::Service	Oui	Non	Oui	Oui	Non	Non	Non
AWS::AppRunner::VpcConnector	Oui	Non	Oui	Oui	Non	Non	Non
AWS::AppStream::Application	Oui	Oui	Oui	Oui	Non	Oui	Non
AWS::AppStream::DirectoryConfig	Oui	Oui	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::AppStream::Fleet	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::AppStream::Stack	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::AppSync::GraphAPI QL	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Athena::DataCatalog	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Athena::PreparedStatement	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Athena::WorkGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::AuditManager::Assessment	Oui	Non	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::AutoScaling::AutoScalingGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::LaunchConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::ScalingPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::ScheduledAction	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::WarmPool	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Backup::BackupPlan	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Backup::BackupSelection	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Backup::BackupVault	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Backup::RecoveryPoint	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Backup::ReportPlan	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Batch::ComputeEnvironment	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Batch::JobQueue	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Batch::SchedulingPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Budgets::BudgetsAction	Non	Non	Oui	Non	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Cassandra::Keyspace	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Cloud9::EnvironmentEC2	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::CloudFormation::Stack	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::CloudFront::Distribution	Non	Non	Oui	Non	Non	Non	Non
AWS::CloudFront::StreamingDistribution	Non	Non	Oui	Non	Non	Non	Non
AWS::CloudTrail::Trail	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::CloudWatch::Alarm	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::CloudWatch::MetricStream	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::CodeArtifact::Repository	Oui	Non	Oui	Oui	Non	Non	Non
AWS::CodeBuild::Project	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::CodeBuild::ReportGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::CodeDeploy::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::CodeDeploy::DeploymentConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::CodeDeploy::DeploymentGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::CodeGuruProfiler::ProfilingGroup	Oui	Non	Oui	Oui	Non	Non	Non
AWS::CodeGuruReviewer::RepositoryAssociation	Oui	Non	Oui	Oui	Non	Non	Non
AWS::CodePipeline::Pipeline	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Cognito::UserPool	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Cognito::UserPoolCliente	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Cognito::User PoolGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Config::ConfigurationRecorder	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Config::ConformancePackConformité	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Config::ResourceCompliance	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Connect::Instance	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Connect::PhoneNumber	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Connect::QuickConnect	Non	Non	Oui	Oui	Non	Oui	Non
AWS::CustomerProfiles::Domain	Non	Non	Oui	Oui	Non	Oui	Non
AWS::CustomerProfiles::ObjectType	Non	Non	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::DMS::Certificate	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DMS::Endpoint	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DMS::EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DMS::ReplicationInstance	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DMS::ReplicationSubnetGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DMS::ReplicationTask	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DataSync::LocationEFS	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::DataSync::LocationF SxLustre	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DataSync::LocationF SxWindows	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Data Sync::LocationHDFS	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DataSync::LocationNFS	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DataSync::LocationObjectRangement	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DataSync::LocationS3	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DataSync::LocationPME	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::DataSync::Task	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Detective::Graph	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::DeviceFarm::InstanceProfile	Non	Non	Non	Oui	Non	Non	Non
AWS::DeviceFarm::Project	Non	Non	Non	Oui	Non	Non	Non
AWS::DeviceFarm::TestGridProjet	Non	Non	Non	Oui	Non	Non	Non
AWS::DynamoDB::Table	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Capacity Reservation	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EC2::CarrierGateway	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::EC2::ClientVpnPoint final	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::CustomerGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::DHCPOptions	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::EC2Fleet	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::EIP	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::EgressOnlyInternetGateway	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EC2::FlowLog	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::Host	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::IPAM	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::IPAMPool	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::IPAMScope	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::Instance	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::InternetGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EC2::LaunchTemplate	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::NatGateway	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::NetworkAcl	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::NetworkInsightsAccessScope	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::NetworkInsightsAccessScopeAnalyse	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::NetworkInsightsAnalyse	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::NetworkInsightsParcours	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EC2::NetworkInterface	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::PrefixList	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::RegisteredInstance de HA	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::RouteTable	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::SecurityGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::SpotFleet	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::Subnet	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EC2::SubnetRouteTableAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::TrafficMirrorFiltre	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::TrafficMirrorSéance	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::TrafficMirrorCible	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::TransitGateway	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::TransitGatewayPièce jointe	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::TransitGatewayConnect	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EC2::TransitGatewayMulticastDomain	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::TransitGatewayRouteTable	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EC2::VPC	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::VPCEndpoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :EC2 : :VPC EndpointService	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :EC2 : :VPC PeeringConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::VPNConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EC2::VPNGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Volume	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECR::PublicRepository	Non	Non	Oui	Non	Non	Non	Non
AWS::ECR::PullThroughCacheRule	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ECR::RegistryPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ECR::Repository	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ECS::CapacityProvider	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::ECS::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::Service	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::TaskDefinition	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::TaskSet	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EFS::AccessPoint	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EFS::FileSystem	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EKS::Addon	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EKS::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EKS::FargateProfile	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EKS::IdentityProviderConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EMR::SecurityConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ElasticBeanstalk::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ElasticBeanstalk::ApplicationVersion	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ElasticBeanstalk::Environment	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::ElasticLoadBalancing::LoadBalancer	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ElasticLoadBalancingV2::Listener	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ElasticLoadBalancingV2::LoadBalancer	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Elasticsearch::Domain	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EventSchemas::Discoverer	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EventSchemas::Registry	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::EventSchemas::RegistryPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::EventSchemas::Schema	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Events::ApiDestination	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Events::Archive	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Events::Connection	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Events::Endpoint	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Events::EventBus	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Events::Rule	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Evidently::Launch	Oui	Non	Oui	Oui	Non	Non	Non
AWS::Evidently::Project	Oui	Non	Oui	Oui	Non	Non	Non
AWS::Evidently::Segment	Oui	Non	Oui	Oui	Non	Non	Non
AWS::FIS::ExperimentTemplate	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Forecast::Dataset	Oui	Non	Oui	Oui	Non	Non	Non
AWS::Forecast::DatasetGroup	Oui	Non	Oui	Oui	Non	Non	Non
AWS::FraudDetector::EntityType	Oui	Non	Oui	Oui	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::FraudDetector::Label	Oui	Non	Oui	Oui	Non	Non	Non
AWS::FraudDetector::Outcome	Oui	Non	Oui	Oui	Non	Non	Non
AWS::FraudDetector::Variable	Oui	Non	Oui	Oui	Non	Non	Non
AWS::GlobalAccelerator::Accelerator	Non	Non	Non	Oui	Non	Non	Non
AWS::GlobalAccelerator::EndpointGroup	Non	Non	Non	Oui	Non	Non	Non
AWS::GlobalAccelerator::Listener	Non	Non	Non	Oui	Non	Non	Non
AWS::Glue::Classifier	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Glue::Job	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Glue::MLTransform	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Grafana::Workspace	Oui	Non	Oui	Oui	Non	Non	Non
AWS::GreengrassV2::ComponentVersion	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::GroundStation::Config	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::GroundStation::DataflowEndpointGroupe	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::GroundStation::MissionProfile	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::GuardDuty::Detector	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::GuardDuty::Filter	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::GuardDevoir : IPSet	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::GuardDuty::ThreatIntelSet	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::HealthLake : :FHIR DataStore	Oui	Non	Oui	Oui	Non	Non	Non
AWS::IAM::Group	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IAM::InstanceProfile	Non	Non	Oui	Non	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::IAM::OIDCProvider	Non	Non	Oui	Non	Non	Non	Non
AWS::IAM::Policy	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IAM::Role	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IAM::SAMLProvider	Non	Non	Oui	Non	Non	Non	Non
AWS::IAM::ServerCertificate	Non	Non	Oui	Non	Non	Non	Non
AWS::IAM::User	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IVS::Channel	Non	Non	Oui	Oui	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::IVS::PlaybackKeyPaire	Non	Non	Oui	Oui	Non	Non	Non
AWS::IVS::RecordingConfiguration	Non	Non	Oui	Oui	Non	Non	Non
AWS::ImageBuilder::ContainerRecipe	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ImageBuilder::DistributionConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ImageBuilder::ImagePipeline	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ImageBuilder::ImageRecipe	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ImageBuilder::InfrastructureConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::InspectorV2::Filter	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IoT::AccountAuditConfiguration	Oui	Non	Oui	Oui	Oui	Oui	Non
AWS::IoT::Authorizer	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IoCertificat T : :CA	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IoT::CustomMetric	Oui	Non	Oui	Oui	Oui	Oui	Non
AWS::IoT::Dimension	Oui	Non	Oui	Oui	Oui	Oui	Non
AWS::IoT::FleetMetric	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::IoT::JobTemplate	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IoT::MitigationAction	Oui	Non	Oui	Oui	Oui	Oui	Non
AWS::IoT::Policy	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IoT::ProvisioningTemplate	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IoT::RoleAlias	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::IoT::ScheduledAudit	Oui	Non	Oui	Oui	Oui	Oui	Non
AWS::IoT::SecurityProfile	Oui	Non	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::IoTAnalytics::Channel	Oui	Non	Oui	Oui	Non	Non	Non
AWS::IoTAnalytics::Dataset	Oui	Non	Oui	Oui	Non	Non	Non
AWS::IoTAnalytics::Datastore	Oui	Non	Oui	Oui	Non	Non	Non
AWS::IoTAnalytics::Pipeline	Oui	Non	Oui	Oui	Non	Non	Non
AWS::IoTEvents::AlarmModel	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::IoTEvents::DetectorModel	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::IoTEvents::Input	Oui	Non	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::IoTSiteWise::AssetModel	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::IoTSiteWise::Dashboard	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::IoTSiteWise::Gateway	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::IoTSiteWise::Portal	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::IoTSiteWise::Project	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::IoTTwinMaker::ComponentType	Non	Non	Oui	Oui	Non	Non	Non
AWS::IoTTwinMaker::Entity	Non	Non	Oui	Oui	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::IoTTwinMaker::Scene	Non	Non	Oui	Oui	Non	Non	Non
AWS::IoTTwinMaker::SyncJob	Non	Non	Oui	Oui	Non	Non	Non
AWS::IoTTwinMaker::Workspace	Non	Non	Oui	Oui	Non	Non	Non
AWS::IoTWireless::FuotaTask	Non	Oui	Oui	Oui	Non	Non	Non
AWS::IoTWireless::MulticastGroup	Non	Oui	Oui	Oui	Non	Non	Non
AWS::IoTWireless::ServiceProfile	Non	Oui	Oui	Oui	Non	Non	Non
AWS::KMS::Alias	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::KMS::Key	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::KafkaConnect::Connector	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Kendra::Index	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Kinesis::Stream	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Kinesis::StreamConsumer	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::KinesisAnalyticsV2::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::KinesisFirehose::DeliveryStream	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::KinesisVideo::SignalingChannel	Oui	Oui	Oui	Oui	Non	Oui	Non
AWS::KinesisVideo::Stream	Oui	Oui	Oui	Oui	Non	Oui	Non
AWS::Lambda::CodeSigningConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Lambda::Function	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Lex::Bot	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Lex::BotAlias	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Lightsail::Bucket	Oui	Non	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Lightsail::Certificate	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Lightsail::Disk	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Lightsail::StaticIp	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Logs::Destination	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::LookoutMetrics::Alert	Oui	Non	Oui	Oui	Non	Non	Non
AWS::LookoutVision::Project	Oui	Non	Oui	Oui	Non	Non	Non
AWS::M2::Environment	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::MSK::BatchScramSecret	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::MSK::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::MSK::ClusterPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::MSK::Configuration	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::MSK::VpcConnection	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::MediaConnect::FlowEntitlement	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::MediaConnect::FlowSource	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::MediaConnect::FlowVpcInterface	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::MediaPackage::PackagingConfiguration	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::MediaPackage::PackagingGroup	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::MediaTailor::PlaybackConfiguration	Oui	Non	Oui	Oui	Non	Non	Non
AWS::MemoryDB::SubnetGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::NetworkFirewall::Firewall	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::NetworkFirewall::FirewallPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::NetworkFirewall::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::NetworkPare-feu : :TLS InspectionConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::NetworkManager::ConnectPeer	Non	Non	Non	Oui	Non	Non	Non
AWS::NetworkManager::CustomerGatewayAssociation	Non	Non	Non	Oui	Non	Non	Non
AWS::NetworkManager::Device	Non	Non	Non	Oui	Non	Non	Non
AWS::NetworkManager::GlobalNetwork	Non	Non	Non	Oui	Non	Non	Non
AWS::NetworkManager::Link	Non	Non	Non	Oui	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::NetworkManager::LinkAssociation	Non	Non	Non	Oui	Non	Non	Non
AWS::NetworkManager::Site	Non	Non	Non	Oui	Non	Non	Non
AWS::NetworkManager::TransitGatewayInscription	Non	Non	Non	Oui	Non	Non	Non
AWS::OpenSearch::Domain	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Panorama::Package	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Personalize::Dataset	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Personalize::DatasetGroup	Oui	Non	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Personalize::Schema	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Personalize::Solution	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Pinpoint::App	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Pinpoint::ApplicationSettings	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Pinpoint::Campaign	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Pinpoint::EmailChannel	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Pinpoint::EmailTemplate	Non	Non	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Pinpoint::EventStream	Non	Non	Oui	Oui	Non	Oui	Non
AWS::Pinpoint::InAppModèle	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::Pinpoint::Segment	Non	Non	Oui	Oui	Non	Oui	Non
AWS::QLDB::Ledger	Oui	Non	Oui	Oui	Non	Oui	Non
AWS::QuickSight::DataSource	Oui	Oui	Oui	Oui	Non	Oui	Non
AWS::QuickSight::Template	Oui	Oui	Oui	Oui	Non	Oui	Non
AWS::QuickSight::Theme	Oui	Oui	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::RDS::DBCluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :RDS : :DB ClusterSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS::DBInstance	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SecurityGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS::DBSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SubnetGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS::EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::RDS::GlobalCluster	Oui	Non	Oui	Oui	Oui	Oui	Non
AWS::RDS::OptionGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::RUM::AppMonitor	Oui	Non	Oui	Oui	Non	Non	Non
AWS::Redshift::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterParameterGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSecurityGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Redshift::ClusterSubnetGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::EndpointAccess	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Redshift::EndpointAuthorization	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Redshift::EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ScheduledAction	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ResilienceHub::App	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ResilienceHub::ResiliencyPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::ResourceExplorer2::Index	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::RoboMaker::RobotApplication	Oui	Non	Oui	Oui	Non	Non	Non
AWS::RoboMaker::RobotApplicationVersion	Oui	Non	Oui	Oui	Non	Non	Non
AWS::RoboMaker::SimulationApplication	Oui	Non	Oui	Oui	Non	Non	Non
AWS::Route53::HealthCheck	Non	Non	Oui	Non	Non	Non	Non
AWS::Route53::HostedZone	Non	Non	Oui	Non	Non	Non	Non
AWS::Route53RecoveryControl::Cluster	Non	Non	Non	Oui	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Route53RecoveryControl::ControlPanel	Non	Non	Non	Oui	Non	Non	Non
AWS::Route53RecoveryControl::RoutingControl	Non	Non	Non	Oui	Non	Non	Non
AWS::Route53RecoveryControl::SafetyRule	Non	Non	Non	Oui	Non	Non	Non
AWS::Route53RecoveryReadiness::Cell	Non	Non	Non	Oui	Non	Non	Non
AWS::Route53RecoveryReadiness::ReadinessCheck	Non	Non	Non	Oui	Non	Non	Non
AWS::Route53RecoveryReadiness::RecoveryGroup	Non	Non	Non	Oui	Non	Non	Non
AWS::Route53RecoveryReadiness::ResourceSet	Non	Non	Non	Oui	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Route53Resolver::FirewallDomainListe	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Route53Resolver::FirewallRuleGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Route53Resolver::FirewallRuleGroupAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Route53Resolver::ResolverEndpoint	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Route53Resolver::ResolverQueryLoggingConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Route53Resolver::ResolverRule	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Route53Resolver::ResolverRuleAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::S3::AccessPoint	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::S3::AccountPublicAccessBlock	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::S3::Bucket	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::S3::MultiRegionAccessPoint	Non	Non	Non	Oui	Non	Non	Non
AWS::S3::StorageLens	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SES::ConfigurationSet	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::SES::ContactList	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SES::ReceiptFilter	Non	Non	Oui	Oui	Non	Non	Non
AWS::SES::ReceiptRuleSet	Non	Non	Oui	Oui	Non	Non	Non
AWS::SES::Template	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SNS::Topic	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::SQS::Queue	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SSM::AssociationCompliance	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::SSM::Document	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SSM::FileData	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SSM::ManagedInstanceInventaire	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SSM::PatchCompliance	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::AppImageConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::CodeRepository	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::Domain	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::SageMaker::EndpointConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::FeatureGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::Image	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::Model	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::NotebookInstance	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::NotebookInstanceLifecycleConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::SageMaker::Workteam	Oui	Non	Oui	Oui	Non	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::SecretsManager::Secret	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ServiceCatalog::CloudFormationProduit	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ServiceCatalog::Portfolio	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ServiceDiscovery::HttpNamespace	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ServiceDiscovery::Instance	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::ServiceDiscovery::PublicDnsEspace de noms	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::ServiceDiscovery::Service	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Shield::Protection	Non	Non	Oui	Non	Non	Non	Non
AWS::ShieldRegional::Protection	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Signer::SigningProfile	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::StepFunctions::Activity	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::StepFunctions::StateMachine	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Transfer::Agreement	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::Transfer::Certificate	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Transfer::Connector	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Transfer::Profile	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::Transfer::Workflow	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAF::RateBasedRègle	Non	Non	Oui	Non	Non	Non	Non
AWS::WAF::Rule	Non	Non	Oui	Non	Non	Non	Non
AWS::WAF::RuleGroup	Non	Non	Oui	Non	Non	Non	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::WAF::WebACL	Non	Non	Oui	Non	Non	Non	Non
AWS::WAFRegional::RateBasedRègle	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAFRegional::Rule	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAFRegional::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAFRegional::WebACL	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAFv2::IPSet	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAFv2::ManagedRuleSet	Oui	Oui	Oui	Oui	Oui	Oui	Non

Type de ressource	USA Ouest (Californie du Nord)	USA Est (Virginie du Nord)	USA Oues (Oregon)	USA Est (Ohio)	Canada Ouest (Calgary)	Canada (Centre)	Amérique du Sud (São Paulo)
AWS::WAFv2::RegexPatternSet	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAFv2::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WAFv2::WebACL	Oui	Oui	Oui	Oui	Oui	Oui	Non
AWS::WorkSpaces::ConnectionAlias	Non	Oui	Oui	Oui	Non	Oui	Non
AWS::WorkSpaces::Workspace	Non	Oui	Oui	Oui	Non	Oui	Non
AWS::XRay::EncryptionConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non

Régions Europe

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::ACM::Certificate	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ACMPCA::CertificateAuthority	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ACMPCA::CertificateAuthorityActivation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::APS::RuleGroupsEspace de noms	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::AccessAnalyzer::Analyzer	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AmazonMQ::Broker	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Amplify::App	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Amplify::Branch	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ApiGateway::RestApi	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ApiGateway::Stage	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ApiGatewayV2::Api	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ApiGatewayV2::Stage	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppConfig::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppConfig::ConfigurationProfile	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppConfig::DeploymentStrategy	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::AppConfig::Environment	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppConfig::ExtensionAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppConfig::HostedConfigurationVersion	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppFlow::Flow	Non	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::AppIntegrations::EventIntegration	Non	Non	Non	Oui	Oui	Non	Non	Non
AWS::AppMesh::GatewayRoute	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppMesh::Mesh	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppMesh::Route	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::AppMesh::VirtualGateway	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppMesh::VirtualNode	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppMesh::VirtualRouter	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppMesh::VirtualService	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AppRunner::Service	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::AppRunner::VpcConnector	Non	Non	Oui	Non	Non	Non	Non	Non
AWS::AppStream::Application	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::AppStream::DirectoryConfig	Non	Non	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::AppStream::Fleet	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::AppStream::Stack	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::AppSync::GraphAPI QL	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Athena::DataCatalog	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Athena::PreparedStatement	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Athena::WorkGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::AuditManager::Assessment	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::AutoScaling::AutoScalingGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::AutoScaling::LaunchConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::ScalingPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::ScheduledAction	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::WarmPool	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Backup::BackupPlan	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Backup::BackupSelection	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Backup::BackupVault	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Backup::RecoveryPoint	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Backup::ReportPlan	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Batch::ComputeEnvironment	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Batch::JobQueue	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Batch::SchedulingPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Cassandra::Keyspace	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Cloud9::EnvironmentEC2	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::CloudFormation::Stack	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::CloudTrail::Trail	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::CloudWatch::Alarm	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::CloudWatch::MetricStream	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::CodeArtifact::Repository	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::CodeBuild::Project	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::CodeBuild::ReportGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::CodeDeploy::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::CodeDeploy::DeploymentConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::CodeDeploy::DeploymentGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::CodeGuruProfiler::ProfilingGroup	Oui	Non	Oui	Oui	Oui	Non	Non	Non
AWS::CodeGuruReviewer::RepositoryAssociation	Oui	Non	Oui	Oui	Oui	Non	Non	Non
AWS::CodePipeline::Pipeline	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Cognito::UserPool	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Cognito::UserPoolCliente	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Cognito::UserPoolGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Config::ConfigurationRecorder	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Config::ConformancePackConformité	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Config::ResourceCompliance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Connect::Instance	Non	Non	Non	Oui	Oui	Non	Non	Non
AWS::Connect::PhoneNumber	Non	Non	Non	Oui	Oui	Non	Non	Non
AWS::Connect::QuickConnect	Non	Non	Non	Oui	Oui	Non	Non	Non
AWS::CustomerProfiles::Domain	Non	Non	Non	Oui	Oui	Non	Non	Non
AWS::CustomerProfiles::ObjectType	Non	Non	Non	Oui	Oui	Non	Non	Non
AWS::DMS::Certificate	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DMS::Endpoint	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::DMS::EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DMS::ReplicationInstance	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DMS::ReplicationSubnetGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DMS::ReplicationTask	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DataSync::LocationEFS	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::DataSync::LocationF SxLustre	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DataSync::LocationF SxWindows	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DataSync::LocationHDFS	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Data Sync::LocationNFS	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::DataSync::LocationObjectRangement	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Data Sync::LocationS3	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Data Sync::LocationPME	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::DataSync::Task	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Detective::Graph	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::DynamoDB::Table	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Capacity Reservation	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::EC2::CarrierGateway	Non	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::EC2::ClientVpnPoint final	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::EC2::CustomerGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::DHCPOptions	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::EC2Fleet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::EIP	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::EgressOnlyInternetGateway	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
AWS::EC2::FlowLog	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::EC2::Host	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::IPAM	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::IPAMPool	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::IPAMScope	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Instance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::InternetGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::LaunchTemplate	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::EC2::NatGateway	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::EC2::NetworkAcl	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::NetworkInsightsAccessScope	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::EC2::NetworkInsightsAccessScopeAnalyse	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::EC2::NetworkInsightsAnalyse	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::EC2::NetworkInsightsParcours	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::EC2::NetworkInterface	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::PrefixList	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::RegisteredInstance de HA	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::EC2::RouteTable	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::SecurityGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::SpotFleet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Subnet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::SubnetRouteTableAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::TrafficMirrorFiltre	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::EC2::TrafficMirrorSéance	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::EC2::TrafficMirrorCible	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::EC2::TransitGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::TransitGatewayPièce jointe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::TransitGatewayConnect	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::EC2::TransitGatewayMulticastDomain	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::TransitGatewayRouteTable	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
AWS::EC2::VPC	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::VPCEndpoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :EC2 : :VPC EndpointService	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS : :EC2 : :VPC PeeringConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2: :VPNConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::VPNGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Volume	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECR::PullThroughCacheRule	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECR::RegistryPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECR::Repository	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS: :CapacityProvider	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::ECS::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::Service	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::TaskDefinition	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::TaskSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EFS::AccessPoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EFS::FileSystem	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EKS::Addon	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EKS::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::EKS::FargateProfile	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EKS::IdentityProviderConfig	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EMR::SecurityConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ElasticBeanstalk::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ElasticBeanstalk::ApplicationVersion	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ElasticBeanstalk::Environment	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ElasticLoadBalancing::LoadBalancer	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ElasticLoadBalancingV2::Listener	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::ElasticLoadBalancingV2::LoadBalancer	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Elasticsearch::Domain	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EventSchemas::Discoverer	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::EventSchemas::Registry	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::EventSchemas::RegistryPolicy	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::EventSchemas::Schema	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Events::ApiDestination	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Events::Archive	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Events::Connection	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Events::Endpoint	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Events::EventBus	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Events::Rule	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Evidently::Launch	Oui	Non	Oui	Oui	Non	Non	Non	Non
AWS::Evidently::Project	Oui	Non	Oui	Oui	Non	Non	Non	Non
AWS::Evidently::Segment	Oui	Non	Oui	Oui	Non	Non	Non	Non
AWS::FIS::ExperimentTemplate	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Forecast::Dataset	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::Forecast::DatasetGroup	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::FraudDetector::EntityType	Non	Non	Oui	Non	Non	Non	Non	Non
AWS::FraudDetector::Label	Non	Non	Oui	Non	Non	Non	Non	Non
AWS::FraudDetector::Outcome	Non	Non	Oui	Non	Non	Non	Non	Non
AWS::FraudDetector::Variable	Non	Non	Oui	Non	Non	Non	Non	Non
AWS::Glue::Classifier	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Glue::Job	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Glue::MLTransform	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Grafana::Workspace	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::GreengrassV2::ComponentVersion	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::GroundStation::Config	Oui	Non	Oui	Oui	Non	Non	Non	Non
AWS::GroundStation::DataflowEndpointGroupe	Oui	Non	Oui	Oui	Non	Non	Non	Non
AWS::GroundStation::MissionProfile	Oui	Non	Oui	Oui	Non	Non	Non	Non
AWS::GuardDuty::Detector	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::GuardDuty::Filter	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::GuardDevoir : IPSet	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::GuardDuty::ThreatIntelSet	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::IAM::Group	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::IAM::Policy	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::IAM::Role	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::IAM::User	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::IVS::Channel	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IVS::PlaybackKeyPaire	Non	Non	Oui	Oui	Non	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::IVS::RecordingConfiguration	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::ImageBuilder::ContainerRecipe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ImageBuilder::DistributionConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ImageBuilder::ImagePipeline	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ImageBuilder::ImageRecipe	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ImageBuilder::InfrastructureConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::InspectorV2::Filter	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::IoT::AccountAuditConfiguration	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::IoT::Authorizer	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoCertificat T : :CA	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::CustomMetric	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::Dimension	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::FleetMetric	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::JobTemplate	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::MitigationAction	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::Policy	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::IoT::ProvisioningTemplate	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::RoleAlias	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::ScheduledAudit	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoT::SecurityProfile	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::IoTAnalytics::Channel	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTAnalytics::Dataset	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTAnalytics::Datastore	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTAnalytics::Pipeline	Non	Non	Oui	Oui	Non	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::IoTEvents::AlarmModel	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::IoTEvents::DetectorModel	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::IoTEvents::Input	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::IoTSiteWise::AssetModel	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTSiteWise::Dashboard	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTSiteWise::Gateway	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTSiteWise::Portal	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTSiteWise::Project	Non	Non	Oui	Oui	Non	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::IoTTwinMaker::ComponentType	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTTwinMaker::Entity	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTTwinMaker::Scene	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTTwinMaker::SyncJob	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTTwinMaker::Workspace	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTWireless::FuotaTask	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTWireless::MulticastGroup	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::IoTWireless::ServiceProfile	Non	Non	Oui	Oui	Non	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::KMS::Alias	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::KMS::Key	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::KafkaConnect::Connector	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Kendra::Index	Non	Non	Oui	Non	Oui	Non	Non	Non
AWS::Kinesis::Stream	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Kinesis::StreamConsumer	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::KinesisAnalyticsV2::Application	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::KinesisFirehose::DeliveryStream	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::KinesisVideo::SignalingChannel	Non	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::KinesisVideo::Stream	Non	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Lambda::CodeSigningConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Lambda::Function	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Lex::Bot	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Lex::BotAlias	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Lightsail::Bucket	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Lightsail::Certificate	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Lightsail::Disk	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Lightsail::StaticIp	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Logs::Destination	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::LookoutMetrics::Alert	Oui	Non	Oui	Oui	Non	Non	Non	Non
AWS::LookoutVision::Project	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::M2::Environment	Non	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::MSK::BatchScramSecret	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MSK::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::MSK::ClusterPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MSK::Configuration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MSK::VpcConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MediaConnect::FlowEntitlement	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::MediaConnect::FlowSource	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::MediaConnect::FlowVpcInterface	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::MediaPackage::PackagingConfiguration	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::MediaPackage::PackagingGroup	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::MediaTailor::PlaybackConfiguration	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::MemoryDB::SubnetGroup	Oui	Non	Oui	Oui	Oui	Non	Non	Non
AWS::NetworkFirewall::Firewall	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::NetworkFirewall::FirewallPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::NetworkFirewall::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::NetworkPare-feu : :TLS InspectionConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::OpenSearch::Domain	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Panorama::Package	Non	Non	Oui	Non	Non	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Personalize::Dataset	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::Personalize::DatasetGroup	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::Personalize::Schema	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::Personalize::Solution	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::Pinpoint::App	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Pinpoint::ApplicationSettings	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Pinpoint::Campaign	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Pinpoint::EmailChannel	Non	Non	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Pinpoint::EmailTemplate	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Pinpoint::EventStream	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Pinpoint::InAppModèle	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Pinpoint::Segment	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::QLDB::Ledger	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::QuickSight::DataSource	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::QuickSight::Template	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::QuickSight::Theme	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::RDS::DBCluster	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
AWS : :RDS : :DB ClusterSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS::DBInstance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SecurityGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS::DBSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SubnetGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS: :EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS::GlobalCluster	Non	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::RDS::OptionGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RUM::AppMonitor	Oui	Non	Oui	Oui	Oui	Non	Non	Non
AWS::Redshift::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterParameterGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSecurityGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSubnetGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::EndpointAccess	Oui	Oui	Oui	Oui	Oui	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Redshift::EndpointAuthorization	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::Redshift::EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ScheduledAction	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ResilienceHub::App	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ResilienceHub::ResiliencyPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ResourceExplorer2::Index	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::RoboMaker::RobotApplication	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::RoboMaker::RobotApplicationVersion	Non	Non	Oui	Oui	Non	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::RoboMaker::SimulationApplication	Non	Non	Oui	Oui	Non	Non	Non	Non
AWS::Route53Resolver::FirewallDomainListe	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Route53Resolver::FirewallRuleGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Route53Resolver::FirewallRuleGroupAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Route53Resolver::ResolverEndpoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Route53Resolver::ResolverQueryLoggingConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Route53Resolver::ResolverRule	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Route53Resolver::ResolverRuleAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::S3::AccessPoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::S3::AccountPublicAccessBlock	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::S3::Bucket	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::S3::StorageLens	Oui	Oui	Oui	Oui	Oui	Non	Non	Non
AWS::SES::ConfigurationSet	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SES::ContactList	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SES::ReceiptFilter	Non	Non	Oui	Non	Non	Non	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::SES::ReceiptRuleSet	Non	Non	Oui	Non	Non	Non	Non	Non
AWS::SES::Template	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SNS::Topic	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SQS::Queue	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SSM::AssociationCompliance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::SSM::Document	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::SSM::FileData	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::SSM::ManagedInstanceInventaire	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::SSM::PatchCompliance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::SageMaker::AppImageConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::CodeRepository	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::Domain	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::EndpointConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::FeatureGroup	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::Image	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::Model	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::SageMaker::NotebookInstance	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::NotebookInstanceLifecycleConfig	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::SageMaker::Workteam	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::SecretsManager::Secret	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceCatalog::CloudFormationProduit	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceCatalog::Portfolio	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceDiscovery::HttpNamespace	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::ServiceDiscovery::Instance	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ServiceDiscovery::PublicDnsEspace de noms	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ServiceDiscovery::Service	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::ShieldRegional::Protection	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Signer::SigningProfile	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::StepFunctions::Activity	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::StepFunctions::StateMachine	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Transfer::Agreement	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::Transfer::Certificate	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Transfer::Connector	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::Transfer::Profile	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Transfer::Workflow	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
AWS::WAFRegional::RateBasedRègle	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFRegional::Rule	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFRegional::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFRegional::WebACL	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Europe (Irlande)	Europe (Francfort)	Europe (Londres)	Europe (Paris)	Europe (Stockholm)	Europe (Milan)	Europe (Espagne)	Europe (Zurich)
AWS::WAFv2::IPSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::ManagedRuleSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::RegexPatternSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::WebACL	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WorkSpaces::ConnectionAlias	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::WorkSpaces::Workspace	Non	Non	Oui	Oui	Oui	Non	Non	Non
AWS::XRay::EncryptionConfig	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Régions Asie-Pacifique

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::ACM::Certificate	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ACMPCA::CertificateAuthority	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ACMPCA::CertificateAuthorityActivation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::APS::RuleGroupsEspace de noms	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::AccessAnalyzer::Analyzer	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AmazonMQ::Broker	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Amplify::App	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Amplify::Branch	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::ApiGateway::RestApi	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ApiGateway::Stage	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ApiGatewayV2::Api	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ApiGatewayV2::Stage	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppConfig::Application	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppConfig::ConfigurationProfile	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppConfig::DeploymentStrategy	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppConfig::Environment	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::AppConfig::ExtensionAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppConfig::HostedConfigurationVersion	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AppFlow::Flow	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::AppIntegrations::EventIntegration	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::AppMesh::GatewayRoute	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::AppMesh::Mesh	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::AppMesh::Route	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::AppMesh::VirtualGateway	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::AppMesh::VirtualNode	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::AppMesh::VirtualRouter	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::AppMesh::VirtualService	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::AppRunner::Service	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::AppRunner::VpcConnector	Non	Non	Non	Non	Non	Non	Non	Oui	Non	Non
AWS::AppStream::Application	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::AppStream::DirectoryConfig	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::AppStream::Fleet	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::AppStream::Stack	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::AppSync::GraphAPI QL	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::Athena::DataCatalog	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Athena::PreparedStatement	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Athena::WorkGroup	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::AuditManager::Assessment	Oui	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::AutoScaling::AutoScalingGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::LaunchConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::AutoScaling::ScalingPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::ScheduledAction	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::AutoScaling::WarmPool	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Backup::BackupPlan	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Backup::BackupSelection	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Backup::BackupVault	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Backup::RecoveryPoint	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Backup::ReportPlan	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Batch::ComputeEnvironment	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::Batch::JobQueue	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::Batch::SchedulingPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::Cassandra::Keyspace	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Cloud9::EnvironmentEC2	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::CloudFormation::Stack	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::CloudTrail::Trail	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::CloudWatch::Alarm	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::CloudWatch::MetricStream	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::CodeArtifact::Repository	Oui	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::CodeBuild::Project	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::CodeBuild::ReportGroup	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::CodeDeploy::Application	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::CodeDeploy::DeploymentConfig	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::CodeDeploy::DeploymentGroup	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::CodeGuruProfiler::ProfilingGroup	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::CodeGuruReviewer::RepositoryAssociation	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::CodePipeline::Pipeline	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Cognito::UserPool	Oui	Non	Non	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Cognito::UserPoolCliente	Oui	Non	Non	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Cognito::UserPoolGroupe	Oui	Non	Non	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Config::ConfigurationRecorder	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Config::ConformancePackConformité	Oui	Non	Oui	Non	Oui	Non	Oui	Oui	Oui	Oui
AWS::Config::ResourceCompliance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Connect::Instance	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Connect::PhoneNumber	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Connect::QuickConnect	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::CustomerProfiles::Domain	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::CustomerProfiles::ObjectType	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::DMS::Certificate	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DMS::Endpoint	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DMS::EventSubscription	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::DMS::ReplicationInstance	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DMS::ReplicationSubnetGroupe	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DMS::ReplicationTask	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DataSync::LocationEFS	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DataSync::LocationF SxLustre	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DataSync::LocationF SxWindows	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::DataSync::LocationHDFS	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::DataSync::LocationNFS	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::DataSync::LocationObjectRangement	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::DataSync::LocationS3	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::DataSync::LocationPME	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::DataSync::Task	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Detective::Graph	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::DynamoDB::Table	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Capacity Reservation	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::CarrierGateway	Non	Non	Non	Non	Oui	Non	Non	Oui	Non	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::EC2::ClientVpnPoint final	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::CustomerGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::DHCPOptions	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::EC2Fleet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::EIP	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::EgressOnlyInternetGateway	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::FlowLog	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::Host	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::EC2::IPAM	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::IPAMPool	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::IPAMScope	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Instance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::InternetGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::LaunchTemplate	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::NatGateway	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::NetworkAcl	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::EC2::NetworkInsightsAccessScope	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::NetworkInsightsAccessScopeAnalyse	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::NetworkInsightsAnalyse	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::NetworkInsightsParcours	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::NetworkInterface	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::PrefixList	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::RegisteredInstance H	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::RouteTable	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::EC2::SecurityGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::SpotFleet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Subnet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::SubnetRouteTableAssociation	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::TrafficMirrorFiltre	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::TrafficMirrorSéance	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::TrafficMirrorCible	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EC2::TransitGateway	Oui	Oui	Oui	Oui	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::EC2::TransitGatewayPièce jointe	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::TransitGatewayConnect	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::TransitGatewayMulticastDomain	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::TransitGatewayRouteTable	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::EC2::VPC	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::VPCEndpoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :EC2 : :VPCEndpointService	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :EC2 : :VPCPeeringConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::EC2::VPNConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::VPNGateway	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EC2::Volume	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECR::PullThroughCacheRule	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECR::RegistryPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECR::Repository	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::CapacityProvider	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::ECS::Service	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::TaskDefinition	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ECS::TaskSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EFS::AccessPoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EFS::FileSystem	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EKS::Addon	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EKS::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EKS::FargateProfile	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::EKS::IdentityProviderConfig	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EMR::SecurityConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ElasticBeanstalk::Application	Oui	Oui	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ElasticBeanstalk::ApplicationVersion	Oui	Oui	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ElasticBeanstalk::Environment	Oui	Oui	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ElasticLoadBalancing::LoadBalancer	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ElasticLoadBalancingV2::Listener	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::ElasticLoadBalancingV2::LoadBalancer	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Elasticsearch::Domain	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::EventSchemas::Discoverer	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EventSchemas::Registry	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EventSchemas::RegistryPolicy	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::EventSchemas::Schema	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Events::ApiDestination	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Events::Archive	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::Events::Connection	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Events::Endpoint	Oui	Non	Non	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Events::EventBus	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Events::Rule	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Evidently::Launch	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::Evidently::Project	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::Evidently::Segment	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::FIS::ExperimentTemplate	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Forecast::Dataset	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Forecast::DatasetGroup	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::FraudDetector::EntityType	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::FraudDetector::Label	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::FraudDetector::Outcome	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::FraudDetector::Variable	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::Glue::Classifier	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Glue::Job	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Glue::MLTransform	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Grafana::Workspace	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::GreengrassV2::ComponentVersion	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::GroundStation::Config	Non	Non	Non	Non	Oui	Non	Non	Non	Oui	Oui
AWS::GroundStation::DataflowEndpointGroupe	Non	Non	Non	Non	Oui	Non	Non	Non	Oui	Oui
AWS::GroundStation::MissionProfile	Non	Non	Non	Non	Oui	Non	Non	Non	Oui	Oui
AWS::GuardDuty::Detector	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::GuardDuty::Filter	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::GuardDevoir : IPset	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::GuardDuty::ThreatIntelSet	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::HealthLake : :FHIR DataStore	Oui	Non	Non	Non	Non	Non	Non	Non	Non	Non
AWS::IAM::Group	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::IAM::Policy	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::IAM::Role	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::IAM::User	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::IVS::Channel	Oui	Non	Non	Non	Oui	Non	Non	Oui	Non	Non
AWS::IVS: :PlaybackKeyPaire	Oui	Non	Non	Non	Oui	Non	Non	Oui	Non	Non

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::IVS::RecordingConfiguration	Oui	Non	Non	Non	Oui	Non	Non	Non	Non	Non
AWS::ImageBuilder::ContainerRecipe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ImageBuilder::DistributionConfiguration	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::ImageBuilder::ImagePipeline	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ImageBuilder::ImageRecipe	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::ImageBuilder::InfrastructureConfiguration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::InspectorV2::Filter	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::AccountAuditConfiguration	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::IoT::Authorizer	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoCertificat T : :CA	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::CustomMetric	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::Dimension	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::FleetMetric	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::JobTemplate	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::MitigationAction	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::Policy	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::IoT::ProvisioningTemplate	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::RoleAlias	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::ScheduledAudit	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoT::SecurityProfile	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTAnalytics::Channel	Oui	Non	Non	Non	Non	Non	Non	Oui	Non	Oui
AWS::IoTAnalytics::Dataset	Oui	Non	Non	Non	Non	Non	Non	Oui	Non	Oui
AWS::IoTAnalytics::Datastore	Oui	Non	Non	Non	Non	Non	Non	Oui	Non	Oui
AWS::IoTAnalytics::Pipeline	Oui	Non	Non	Non	Non	Non	Non	Oui	Non	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::IoTEvents::AlarmModel	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTEvents::DetectorModel	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTEvents::Input	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTSiteWise::AssetModel	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTSiteWise::Dashboard	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTSiteWise::Gateway	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTSiteWise::Portal	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::IoTSiteWise::Project	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::IoTTwinMaker::ComponentType	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::IoTTwinMaker::Entity	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::IoTTwinMaker::Scene	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::IoTTwinMaker::SyncJob	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::IoTTwinMaker::Workspace	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui
AWS::IoTWireless::FuotaTask	Non	Non	Non	Non	Non	Non	Non	Oui	Non	Oui
AWS::IoTWireless::MulticastGroup	Non	Non	Non	Non	Non	Non	Non	Oui	Non	Oui
AWS::IoTWireless::ServiceProfile	Non	Non	Non	Non	Non	Non	Non	Oui	Non	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::KMS::Alias	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::KMS::Key	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::KafkaConnect::Connector	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Kendra::Index	Oui	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::Kinesis::Stream	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Kinesis::StreamConsumer	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::KinesisAnalyticsV2::Application	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::KinesisFirehose::DeliveryStream	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::KinesisVideo::SignalingChannel	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::KinesisVideo::Stream	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Lambda::CodeSigningConfig	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Lambda::Function	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Lex::Bot	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Lex::BotAlias	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Lightsail::Bucket	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Lightsail::Certificate	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Lightsail::Disk	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Lightsail::StaticIp	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Logs::Destination	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::LookoutMetrics::Alert	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::LookoutVision::Project	Non	Non	Non	Non	Oui	Non	Non	Oui	Non	Non
AWS::M2::Environment	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::MSK::BatchScramSecret	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MSK::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::MSK::ClusterPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MSK::Configuration	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MSK::VpcConnection	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::MediaConnect::FlowEntitlement	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::MediaConnect::FlowSource	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::MediaConnect::FlowVpcInterface	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::MediaPackage::PackagingConfiguration	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::MediaPackage::PackagingGroup	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::MediaTailor::PlaybackConfiguration	Oui	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::MemoryDB::SubnetGroup	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::NetworkFirewall::Firewall	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::NetworkFirewall::FirewallPolicy	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::NetworkFirewall::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::NetworkPare-feu : :TLS InspectionConfiguration	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::OpenSearch::Domain	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Panorama::Package	Non	Non	Non	Non	Non	Non	Non	Non	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Personalize::Dataset	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Personalize::DatasetGroup	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Personalize::Schema	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Personalize::Solution	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Pinpoint::App	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Pinpoint::ApplicationSettings	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Pinpoint::Campaign	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Pinpoint::EmailChannel	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Pinpoint::EmailTemplate	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Pinpoint::EventStream	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Pinpoint::InAppModèle	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Pinpoint::Segment	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::QLDB::Ledger	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::QuickSight::DataSource	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::QuickSight::Template	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::QuickSight::Theme	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::RDS::DBCluster	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS : :RDS : :DB ClusterSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS: :DBInstance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SecurityGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS: :DBSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SubnetGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS: :EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RDS: :GlobalCluster	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::RDS::OptionGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::RUM::AppMonitor	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Oui
AWS::Redshift::Cluster	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterParameterGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSecurityGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSnapshot	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSubnetGroupe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::EndpointAccess	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Redshift::EndpointAuthorization	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::Redshift::EventSubscription	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Redshift::ScheduledAction	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ResilienceHub::App	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ResilienceHub::ResiliencyPolicy	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ResourceExplorer2::Index	Oui	Non	Non	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::RoboMaker::RobotApplication	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Non
AWS::RoboMaker::RobotApplicationVersion	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Non

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::RoboMaker::SimulationApplication	Non	Non	Non	Non	Non	Non	Non	Oui	Oui	Non
AWS::Route53Resolver::FirewallDomainListe	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Route53Resolver::FirewallRuleGroupe	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Route53Resolver::FirewallRuleGroupAssociation	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Route53Resolver::ResolverEndpoint	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Route53Resolver::ResolverQueryLoggingConfig	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Route53Resolver::ResolverRule	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Route53Resolver::ResolverRuleAssociation	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::S3::AccessPoint	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::S3::AccountPublicAccessBlock	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::S3::Bucket	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::S3::StorageLens	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::SES::ConfigurationSet	Oui	Oui	Non	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SES::ContactList	Oui	Oui	Non	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SES::Template	Oui	Oui	Non	Non	Oui	Oui	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::SNS::Topic	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SQS::Queue	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SSM::AssociationCompliance	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui
AWS::SSM::Document	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::SSM::FileData	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui
AWS::SSM::ManagedInstanceInventaire	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::SSM::PatchCompliance	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui	Oui
AWS::SageMaker::AppImageConfig	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::SageMaker::CodeRepository	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SageMaker::Domain	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SageMaker::EndpointConfig	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SageMaker::FeatureGroup	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SageMaker::Image	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::SageMaker::Model	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SageMaker::NotebookInstance	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::SageMaker::NotebookInstanceLifecycleConfig	Oui	Non	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::SageMaker::Workteam	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::SecretsManager::Secret	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceCatalog::CloudFormationProduit	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceCatalog::Portfolio	Oui	Non	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::ServiceDiscovery::HttpNamespace	Oui	Non	Oui	Non	Oui	Non	Oui	Oui	Oui	Oui
AWS::ServiceDiscovery::Instance	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ServiceDiscovery::PublicDnsEspace de noms	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::ServiceDiscovery::Service	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::ShieldRegional::Protection	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Signer::SigningProfile	Oui	Non	Oui	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::StepFunctions::Activity	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::StepFunctions::StateMachine	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
AWS::Transfer::Agreement	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Transfer::Certificate	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::Transfer::Connector	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::Transfer::Profile	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::Transfer::Workflow	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui	Oui	Oui
AWS::WAFRegional::RateBasedRègle	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFRegional::Rule	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFRegional::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFRegional::WebACL	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::IPSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::ManagedRuleSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Type de ressource	Asie-Pacifique (Singapour)	Asie-Pacifique (Tokyo)	Asie-Pacifique (Sydney)	Asie-Pacifique (Séoul)	Asie-Pacifique (Mumbai)	Asie-Pacifique (Osaka)	Asie-Pacifique (Hong Kong)	Asie-Pacifique (Jakarta)	Asie-Pacifique (Hyderabad)	Asie-Pacifique (Melbourne)
AWS::WAFv2::RegexPatternSet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::RuleGroup	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WAFv2::WebACL	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
AWS::WorkSpaces::ConnectionAlias	Non	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::WorkSpaces::Workspace	Oui	Non	Non	Non	Oui	Non	Non	Oui	Oui	Oui
AWS::XRay::EncryptionConfig	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Régions Chine

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::ACM::Certificate	Oui	Oui
AWS::AmazonMQ::Broker	Oui	Oui
AWS::ApiGateway::RestApi	Oui	Oui
AWS::ApiGateway::Stage	Oui	Oui
AWS::ApiGatewayV2::Api	Oui	Oui
AWS::ApiGatewayV2::Stage	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::AppConfig::Application	Oui	Oui
AWS::AppConfig::ConfigurationProfile	Oui	Oui
AWS::AppConfig::DeploymentStrategy	Oui	Oui
AWS::AppConfig::Environment	Oui	Oui
AWS::AppConfig::ExtensionAssociation	Oui	Oui
AWS::AppConfig::HostedConfigurationVersion	Oui	Oui
AWS::AppSync::GraphAPI QL	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::Athena::DataCatalog	Oui	Oui
AWS::Athena::PreparedStatement	Oui	Oui
AWS::Athena::WorkGroup	Oui	Oui
AWS::AutoScaling::AutoScalingGroupe	Oui	Oui
AWS::AutoScaling::LaunchConfiguration	Oui	Oui
AWS::AutoScaling::ScalingPolicy	Oui	Oui
AWS::AutoScaling::ScheduledAction	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::AutoScaling::WarmPool	Oui	Oui
AWS::Backup::BackupPlan	Oui	Oui
AWS::Backup::BackupSelection	Oui	Oui
AWS::Backup::BackupVault	Oui	Oui
AWS::Backup::RecoveryPoint	Oui	Oui
AWS::Batch::ComputeEnvironment	Oui	Oui
AWS::Batch::JobQueue	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::Batch::SchedulingPolicy	Oui	Oui
AWS::Cassandra::Keyspace	Oui	Oui
AWS::CloudFormation::Stack	Oui	Oui
AWS::CloudTrail::Trail	Oui	Oui
AWS::CloudWatch::Alarm	Oui	Oui
AWS::CloudWatch::MetricStream	Oui	Oui
AWS::CodeBuild::Project	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::CodeBuild::ReportGroup	Oui	Oui
AWS::Config::ConfigurationRecorder	Oui	Oui
AWS::Config::ResourceCompliance	Oui	Oui
AWS::DMS::Certificate	Oui	Oui
AWS::DMS::Endpoint	Oui	Oui
AWS::DMS::EventSubscription	Oui	Oui
AWS::DMS::ReplicationInstance	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::DMS::ReplicationSubnetGroupe	Oui	Oui
AWS::DMS::ReplicationTask	Oui	Oui
AWS::DataSync::LocationEFS	Oui	Oui
AWS::DataSync::LocationHDFS	Oui	Oui
AWS::DataSync::LocationNFS	Oui	Oui
AWS::DataSync::LocationObjectRangement	Oui	Oui
AWS::DataSync::LocationS3	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::DataSync::LocationPME	Oui	Oui
AWS::DataSync::Task	Oui	Oui
AWS::DynamoDB::Table	Oui	Oui
AWS::EC2::CapacityReservation	Oui	Oui
AWS::EC2::DHCPOptions	Oui	Oui
AWS::EC2::EC2Fleet	Oui	Oui
AWS::EC2::EIP	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::EC2::FlowLog	Oui	Oui
AWS::EC2::Host	Oui	Oui
AWS::EC2::Instance	Oui	Oui
AWS::EC2::InternetGateway	Oui	Oui
AWS::EC2::LaunchTemplate	Oui	Oui
AWS::EC2::NatGateway	Oui	Oui
AWS::EC2::NetworkAcl	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::EC2::NetworkInterface	Oui	Oui
AWS::EC2::PrefixList	Oui	Oui
AWS::EC2::RouteTable	Oui	Oui
AWS::EC2::SecurityGroup	Oui	Oui
AWS::EC2::SpotFleet	Oui	Oui
AWS::EC2::Subnet	Oui	Oui
AWS::EC2::SubnetRouteTableAssociation	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::EC2::TrafficMirrorFiltre	Oui	Oui
AWS::EC2::TrafficMirrorSéance	Oui	Oui
AWS::EC2::TrafficMirrorCible	Oui	Oui
AWS::EC2::TransitGateway	Oui	Oui
AWS::EC2::TransitGatewayPièce jointe	Oui	Oui
AWS::EC2::TransitGatewayConnect	Oui	Oui
AWS::EC2::TransitGatewayMulticastDomain	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::EC2::TransitGatewayRouteTable	Oui	Oui
AWS::EC2::VPC	Oui	Oui
AWS::EC2::VPCEndpoint	Oui	Oui
AWS : :EC2 : :VPC EndpointService	Oui	Oui
AWS : :EC2 : :VPC PeeringConnection	Oui	Oui
AWS::EC2::VPNGateway	Oui	Non
AWS::EC2::Volume	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::ECR::Repository	Oui	Oui
AWS::ECS::CapacityProvider	Oui	Oui
AWS::ECS::Cluster	Oui	Oui
AWS::ECS::Service	Oui	Oui
AWS::ECS::TaskDefinition	Oui	Oui
AWS::ECS::TaskSet	Oui	Oui
AWS::EFS::AccessPoint	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::EFS::FileSystem	Oui	Oui
AWS::EKS::Addon	Oui	Oui
AWS::EKS::Cluster	Oui	Oui
AWS::EKS::FargateProfile	Oui	Oui
AWS::EKS::IdentityProviderConfig	Oui	Oui
AWS::EMR::SecurityConfiguration	Oui	Oui
AWS::ElasticBeanstalk::Application	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::ElasticBeanstalk::ApplicationVersion	Oui	Oui
AWS::ElasticBeanstalk::Environment	Oui	Oui
AWS::ElasticLoadBalancing::LoadBalancer	Oui	Oui
AWS::ElasticLoadBalancingV2::Listener	Oui	Oui
AWS::ElasticLoadBalancingV2::LoadBalancer	Oui	Oui
AWS::Elasticsearch::Domain	Oui	Oui
AWS::Events::Archive	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::Events::EventBus	Oui	Oui
AWS::Events::Rule	Oui	Oui
AWS::Glue::Classifier	Oui	Oui
AWS::Glue::Job	Oui	Oui
AWS::Glue::MLTransform	Oui	Non
AWS::GreengrassV2::ComponentVersion	Oui	Non
AWS::GuardDuty::Filter	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::GuardDuty::ThreatIntelSet	Oui	Oui
AWS::IAM::Group	Oui	Oui
AWS::IAM::InstanceProfile	Oui	Non
AWS::IAM::OIDCProvider	Oui	Non
AWS::IAM::Policy	Oui	Oui
AWS::IAM::Role	Oui	Oui
AWS::IAM::SAMLProvider	Oui	Non

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::IAM::ServerCertificate	Oui	Non
AWS::IAM::User	Oui	Oui
AWS::ImageBuilder::ContainerRecipe	Oui	Oui
AWS::ImageBuilder::DistributionConfiguration	Oui	Oui
AWS::ImageBuilder::ImagePipeline	Oui	Oui
AWS::ImageBuilder::ImageRecipe	Oui	Oui
AWS::ImageBuilder::InfrastructureConfiguration	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::IoT::AccountAuditConfiguration	Oui	Oui
AWS::IoT::Authorizer	Oui	Oui
AWS::IoCertificat T : :CA	Oui	Oui
AWS::IoT::CustomMetric	Oui	Oui
AWS::IoT::Dimension	Oui	Oui
AWS::IoT::FleetMetric	Oui	Oui
AWS::IoT::JobTemplate	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::IoT::MitigationAction	Oui	Oui
AWS::IoT::Policy	Oui	Oui
AWS::IoT::ProvisioningTemplate	Oui	Oui
AWS::IoT::RoleAlias	Oui	Oui
AWS::IoT::ScheduledAudit	Oui	Oui
AWS::IoT::SecurityProfile	Oui	Oui
AWS::IoTAnalytics::Channel	Oui	Non

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::IoTAnalytics::Dataset	Oui	Non
AWS::IoTAnalytics::Datastore	Oui	Non
AWS::IoTAnalytics::Pipeline	Oui	Non
AWS::IoTEvents::AlarmModel	Oui	Non
AWS::IoTEvents::DetectorModel	Oui	Non
AWS::IoTEvents::Input	Oui	Non
AWS::IoTSiteWise::AssetModel	Oui	Non

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::IoTSiteWise::Dashboard	Oui	Non
AWS::IoTSiteWise::Gateway	Oui	Non
AWS::IoTSiteWise::Portal	Oui	Non
AWS::IoTSiteWise::Project	Oui	Non
AWS::KMS::Alias	Oui	Oui
AWS::KMS::Key	Oui	Oui
AWS::Kinesis::Stream	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::Kinesis::StreamConsumer	Oui	Oui
AWS::KinesisAnalyticsV2::Application	Oui	Oui
AWS::KinesisFirehose::DeliveryStream	Oui	Oui
AWS::Lambda::Function	Oui	Non
AWS::Logs::Destination	Oui	Oui
AWS::MSK::BatchScramSecret	Oui	Oui
AWS::MSK::Cluster	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::MSK::ClusterPolicy	Oui	Oui
AWS::MSK::Configuration	Oui	Oui
AWS::MSK::VpcConnection	Oui	Oui
AWS::NetworkFirewall::Firewall	Oui	Oui
AWS::NetworkFirewall::FirewallPolicy	Oui	Oui
AWS::NetworkFirewall::RuleGroup	Oui	Oui
AWS::NetworkPare-feu : :TLS InspectionConfiguration	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::OpenSearch::Domain	Oui	Oui
AWS::Personalize::Dataset	Oui	Non
AWS::Personalize::DatasetGroup	Oui	Non
AWS::Personalize::Schema	Oui	Non
AWS::Personalize::Solution	Oui	Non
AWS::RDS::DBCluster	Non	Oui
AWS : :RDS : :DB ClusterSnapshot	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::RDS::DBInstance	Oui	Oui
AWS : :RDS : :DB SecurityGroup	Oui	Oui
AWS::RDS::DBSnapshot	Oui	Oui
AWS : :RDS : :DB SubnetGroup	Oui	Oui
AWS::RDS::EventSubscription	Oui	Oui
AWS::RDS::OptionGroup	Oui	Oui
AWS::Redshift::Cluster	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::Redshift::ClusterParameterGroupe	Oui	Oui
AWS::Redshift::ClusterSecurityGroupe	Oui	Oui
AWS::Redshift::ClusterSnapshot	Oui	Oui
AWS::Redshift::ClusterSubnetGroupe	Oui	Oui
AWS::Redshift::EventSubscription	Oui	Oui
AWS::Route53Resolver::FirewallDomainListe	Oui	Oui
AWS::Route53Resolver::FirewallRuleGroupAssociation	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::Route53Resolver::ResolverEndpoint	Oui	Oui
AWS::Route53Resolver::ResolverQueryLoggingConfig	Oui	Oui
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Oui	Oui
AWS::Route53Resolver::ResolverRule	Oui	Oui
AWS::Route53Resolver::ResolverRuleAssociation	Oui	Oui
AWS::S3::AccessPoint	Oui	Oui
AWS::S3::AccountPublicAccessBlock	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::S3::Bucket	Oui	Oui
AWS::SES::ConfigurationSet	Non	Oui
AWS::SES::ContactList	Non	Oui
AWS::SES::Template	Non	Oui
AWS::SNS::Topic	Oui	Oui
AWS::SQS::Queue	Oui	Oui
AWS::SSM::AssociationCompliance	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::SSM::Document	Oui	Oui
AWS::SSM::FileData	Oui	Oui
AWS::SSM::ManagedInstanceInventaire	Oui	Oui
AWS::SSM::PatchCompliance	Oui	Oui
AWS::SageMaker::AppImageConfig	Oui	Oui
AWS::SageMaker::CodeRepository	Oui	Oui
AWS::SageMaker::Domain	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::SageMaker::EndpointConfig	Oui	Oui
AWS::SageMaker::FeatureGroup	Oui	Oui
AWS::SageMaker::Image	Oui	Oui
AWS::SageMaker::Model	Oui	Oui
AWS::SageMaker::NotebookInstance	Oui	Oui
AWS::SageMaker::NotebookInstanceLifecycleConfig	Oui	Oui
AWS::SecretsManager::Secret	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::ServiceCatalog::CloudFormationProduit	Oui	Oui
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Oui	Oui
AWS::ServiceCatalog::Portfolio	Oui	Oui
AWS::ServiceDiscovery::HttpNamespace	Oui	Oui
AWS::ServiceDiscovery::Instance	Oui	Oui
AWS::ServiceDiscovery::PublicDnsEspace de noms	Oui	Oui
AWS::ServiceDiscovery::Service	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::StepFunctions::Activity	Oui	Non
AWS::StepFunctions::StateMachine	Oui	Oui
AWS::Transfer::Agreement	Oui	Oui
AWS::Transfer::Certificate	Oui	Oui
AWS::Transfer::Connector	Oui	Oui
AWS::Transfer::Profile	Oui	Oui
AWS::Transfer::Workflow	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::WAFRegional::RateBasedRègle	Oui	Oui
AWS::WAFRegional::Rule	Oui	Oui
AWS::WAFRegional::RuleGroup	Oui	Oui
AWS::WAFRegional::WebACL	Oui	Oui
AWS::WAFv2::IPSet	Oui	Oui
AWS::WAFv2::ManagedRuleSet	Oui	Oui
AWS::WAFv2::RegexPatternSet	Oui	Oui

Type de ressource	Chine (Beijing)	Chine (Ningxia)
AWS::WAFv2::RuleGroup	Oui	Oui
AWS::WAFv2::WebACL	Oui	Oui
AWS::WorkSpaces::Workspace	Non	Oui

Régions Afrique et Moyen-Orient

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ACM::Certificate	Oui	Oui	Oui	Oui
AWS::ACMPCA::CertificateAuthority	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ACMPCA::CertificateAuthorityActivation	Oui	Oui	Oui	Non
AWS::AccessAnalyzer::Analyzer	Oui	Oui	Oui	Non
AWS::AmazonMQ::Broker	Oui	Oui	Oui	Non
AWS::Amplify::App	Oui	Non	Non	Non
AWS::Amplify::Branch	Oui	Non	Non	Non
AWS::ApiGateway::RestApi	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ApiGateway::Stage	Oui	Oui	Oui	Oui
AWS::ApiGatewayV2::Api	Oui	Oui	Oui	Oui
AWS::ApiGatewayV2::Stage	Oui	Oui	Oui	Oui
AWS::AppConfig::Application	Oui	Oui	Non	Oui
AWS::AppConfig::ConfigurationProfile	Oui	Oui	Non	Oui
AWS::AppConfig::DeploymentStrategy	Oui	Oui	Non	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::AppConfig::Environment	Oui	Oui	Non	Oui
AWS::AppConfig::ExtensionAssociation	Oui	Oui	Oui	Oui
AWS::AppConfig::HostedConfigurationVersion	Oui	Oui	Non	Oui
AWS::AppIntegrations::EventIntegration	Non	Oui	Non	Non
AWS::AppMesh::GatewayRoute	Oui	Oui	Non	Non
AWS::AppMesh::Mesh	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::AppMesh::Route	Oui	Oui	Non	Non
AWS::AppMesh::VirtualGateway	Oui	Oui	Non	Non
AWS::AppMesh::VirtualNode	Oui	Oui	Non	Non
AWS::AppMesh::VirtualRouter	Oui	Oui	Non	Non
AWS::AppMesh::VirtualService	Oui	Oui	Non	Non
AWS::AppSync::GraphAPI QL	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::Athena::DataCatalog	Oui	Oui	Oui	Non
AWS::Athena::PreparedStatement	Oui	Oui	Non	Non
AWS::Athena::WorkGroup	Oui	Oui	Oui	Non
AWS::AutoScaling::AutoScalingGroupe	Oui	Oui	Oui	Oui
AWS::AutoScaling::LaunchConfiguration	Oui	Oui	Oui	Oui
AWS::AutoScaling::ScalingPolicy	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::AutoScaling::ScheduledAction	Oui	Oui	Oui	Oui
AWS::AutoScaling::WarmPool	Oui	Oui	Non	Non
AWS::Backup::BackupPlan	Oui	Oui	Non	Non
AWS::Backup::BackupSelection	Oui	Oui	Oui	Non
AWS::Backup::BackupVault	Oui	Oui	Oui	Non
AWS::Backup::RecoveryPoint	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::Backup::ReportPlan	Oui	Oui	Non	Non
AWS::Batch::ComputeEnvironment	Oui	Oui	Oui	Non
AWS::Batch::JobQueue	Oui	Oui	Oui	Non
AWS::Batch::SchedulingPolicy	Oui	Oui	Oui	Non
AWS::Cassandra::Keyspace	Oui	Non	Non	Non
AWS::Cloud9::EnvironmentEC2	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::CloudFormation::Stack	Oui	Oui	Non	Non
AWS::CloudTrail::Trail	Oui	Oui	Oui	Oui
AWS::CloudWatch::Alarm	Oui	Oui	Oui	Oui
AWS::CloudWatch::MetricStream	Oui	Oui	Oui	Oui
AWS::CodeBuild::Project	Oui	Oui	Oui	Oui
AWS::CodeBuild::ReportGroup	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::CodeDeploy::Application	Oui	Oui	Non	Non
AWS::CodeDeploy::DeploymentConfig	Oui	Oui	Non	Non
AWS::CodeDeploy::DeploymentGroup	Oui	Oui	Non	Non
AWS::Cognito::UserPool	Oui	Non	Non	Oui
AWS::Cognito::UserPoolCliente	Oui	Non	Non	Oui
AWS::Cognito::UserPoolGroupe	Oui	Non	Non	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::Config::ConfigurationRecorder	Oui	Oui	Oui	Oui
AWS::Config::ConformancePackConformité	Oui	Non	Non	Non
AWS::Config::ResourceCompliance	Oui	Oui	Oui	Oui
AWS::Connect::Instance	Non	Oui	Non	Non
AWS::CustomerProfiles::Domain	Non	Oui	Non	Non
AWS::CustomerProfiles::ObjectType	Non	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::DMS::Certificate	Oui	Oui	Non	Non
AWS::DMS::Endpoint	Oui	Oui	Non	Non
AWS::DMS::EventSubscription	Oui	Oui	Non	Non
AWS::DMS::ReplicationInstance	Oui	Oui	Non	Non
AWS::DMS::ReplicationSubnetGroupe	Oui	Oui	Non	Non
AWS::DMS::ReplicationTask	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::DataSync::LocationEFS	Oui	Oui	Oui	Non
AWS::DataSync::LocationF SxLustre	Oui	Oui	Non	Non
AWS::DataSync::LocationF SxWindows	Oui	Oui	Non	Non
AWS::DataSync::LocationHDFS	Oui	Oui	Oui	Non
AWS::DataSync::LocationNFS	Oui	Oui	Oui	Non
AWS::DataSync::LocationObjectRangement	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::DataSync::LocationS3	Oui	Oui	Oui	Non
AWS::DataSync::LocationPME	Oui	Oui	Oui	Non
AWS::DataSync::Task	Oui	Oui	Oui	Non
AWS::Detective::Graph	Oui	Oui	Non	Non
AWS::DynamoDB::Table	Oui	Oui	Oui	Oui
AWS::EC2::CapacityReservation	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EC2::ClientVpnPoint final	Oui	Oui	Non	Non
AWS::EC2::CustomerGateway	Oui	Oui	Oui	Oui
AWS::EC2::DHCPOptions	Oui	Oui	Oui	Oui
AWS::EC2::EC2Fleet	Oui	Oui	Oui	Non
AWS::EC2::EIP	Oui	Oui	Oui	Oui
AWS::EC2::EgressOnlyInternetGateway	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EC2::FlowLog	Oui	Oui	Oui	Non
AWS::EC2::Host	Oui	Oui	Oui	Oui
AWS::EC2::IPAM	Oui	Oui	Oui	Non
AWS::EC2::IPAMPool	Oui	Oui	Oui	Non
AWS::EC2::IPAMScope	Oui	Oui	Oui	Non
AWS::EC2::Instance	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EC2::InternetGateway	Oui	Oui	Oui	Oui
AWS::EC2::LaunchTemplate	Oui	Oui	Non	Non
AWS::EC2::NatGateway	Oui	Oui	Oui	Non
AWS::EC2::NetworkAcl	Oui	Oui	Oui	Oui
AWS::EC2::NetworkInsightsAccessScope	Oui	Oui	Non	Non
AWS::EC2::NetworkInsightsAccessScopeAnalyse	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EC2::NetworkInsightsAnalyse	Oui	Oui	Non	Non
AWS::EC2::NetworkInsightsParcours	Oui	Oui	Non	Non
AWS::EC2::NetworkInterface	Oui	Oui	Oui	Oui
AWS::EC2::PrefixList	Oui	Oui	Oui	Oui
AWS::EC2::RouteTable	Oui	Oui	Oui	Oui
AWS::EC2::SecurityGroup	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EC2::SpotFleet	Oui	Oui	Oui	Oui
AWS::EC2::Subnet	Oui	Oui	Oui	Oui
AWS::EC2::SubnetRouteTableAssociation	Oui	Oui	Oui	Oui
AWS::EC2::TrafficMirrorFiltre	Oui	Non	Non	Non
AWS::EC2::TrafficMirrorSéance	Oui	Non	Non	Non
AWS::EC2::TrafficMirrorCible	Oui	Non	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EC2::TransitGateway	Oui	Oui	Oui	Non
AWS::EC2::TransitGatewayPièce jointe	Oui	Oui	Oui	Non
AWS::EC2::TransitGatewayConnect	Oui	Oui	Oui	Non
AWS::EC2::TransitGatewayMulticastDomain	Oui	Oui	Oui	Oui
AWS::EC2::TransitGatewayRouteTable	Oui	Oui	Oui	Non
AWS::EC2::VPC	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EC2::VPCEndpoint	Oui	Oui	Oui	Oui
AWS : :EC2 : :VPC EndpointService	Oui	Oui	Oui	Oui
AWS : :EC2 : :VPC PeeringConnection	Oui	Oui	Oui	Oui
AWS::EC2::VPNConnection	Oui	Oui	Oui	Oui
AWS::EC2::VPNGateway	Oui	Oui	Oui	Oui
AWS::EC2::Volume	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ECR::PullThroughCacheRule	Oui	Oui	Oui	Oui
AWS::ECR::RegistryPolicy	Oui	Oui	Oui	Non
AWS::ECR::Repository	Oui	Oui	Oui	Non
AWS::ECS::CapacityProvider	Oui	Oui	Oui	Oui
AWS::ECS::Cluster	Oui	Oui	Oui	Oui
AWS::ECS::Service	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ECS::TaskDefinition	Oui	Oui	Oui	Oui
AWS::ECS::TaskSet	Oui	Oui	Oui	Non
AWS::EFS::AccessPoint	Oui	Oui	Oui	Non
AWS::EFS::FileSystem	Oui	Oui	Oui	Non
AWS::EKS::Addon	Oui	Oui	Oui	Non
AWS::EKS::Cluster	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::EKS::FargateProfile	Oui	Oui	Oui	Oui
AWS::EKS::IdentityProviderConfig	Oui	Oui	Oui	Non
AWS::EMR::SecurityConfiguration	Oui	Oui	Oui	Non
AWS::ElasticBeanstalk::Application	Non	Oui	Non	Non
AWS::ElasticBeanstalk::ApplicationVersion	Non	Oui	Non	Non
AWS::ElasticBeanstalk::Environment	Non	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ElasticLoadBalancing::LoadBalancer	Oui	Oui	Oui	Oui
AWS::ElasticLoadBalancingV2::Listener	Oui	Oui	Non	Non
AWS::ElasticLoadBalancingV2::LoadBalancer	Oui	Oui	Oui	Oui
AWS::Elasticsearch::Domain	Oui	Oui	Oui	Oui
AWS::Events::ApiDestination	Oui	Oui	Non	Non
AWS::Events::Archive	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::Events::Connection	Oui	Oui	Non	Non
AWS::Events::EventBus	Oui	Oui	Non	Non
AWS::Events::Rule	Oui	Oui	Non	Non
AWS::FIS::ExperimentTemplate	Oui	Oui	Non	Non
AWS::Glue::Classifier	Oui	Oui	Oui	Oui
AWS::Glue::Job	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::Glue::MLTransform	Oui	Oui	Oui	Oui
AWS::GroundStation::Config	Oui	Oui	Non	Non
AWS::GroundStation ::DataflowEndpointGroupe	Oui	Oui	Non	Non
AWS::GroundStation::MissionProfile	Oui	Oui	Non	Non
AWS::GuardDuty::Detector	Oui	Oui	Non	Non
AWS::GuardDuty::Filter	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::GuardDevoir : IPset	Oui	Oui	Non	Non
AWS::GuardDuty::ThreatIntelSet	Oui	Oui	Non	Non
AWS::IAM::Group	Oui	Oui	Non	Non
AWS::IAM::Policy	Oui	Oui	Non	Non
AWS::IAM::Role	Oui	Oui	Non	Non
AWS::IAM::User	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ImageBuilder::ContainerRecipe	Oui	Oui	Oui	Oui
AWS::ImageBuilder::DistributionConfiguration	Oui	Oui	Non	Non
AWS::ImageBuilder::ImagePipeline	Oui	Oui	Oui	Oui
AWS::ImageBuilder::ImageRecipe	Oui	Oui	Non	Non
AWS::ImageBuilder::InfrastructureConfiguration	Oui	Oui	Oui	Oui
AWS::InspectorV2::Filter	Oui	Non	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::IoT::AccountAuditConfiguration	Oui	Non	Oui	Non
AWS::IoT::Authorizer	Oui	Non	Oui	Non
AWS::IoCertificat T : :CA	Oui	Non	Oui	Non
AWS::IoT::CustomMetric	Oui	Non	Oui	Non
AWS::IoT::Dimension	Oui	Non	Oui	Non
AWS::IoT::FleetMetric	Oui	Non	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::IoT::JobTemplate	Oui	Non	Oui	Non
AWS::IoT::MitigationAction	Oui	Non	Oui	Non
AWS::IoT::Policy	Oui	Non	Oui	Non
AWS::IoT::ProvisioningTemplate	Oui	Non	Oui	Non
AWS::IoT::RoleAlias	Oui	Non	Oui	Non
AWS::IoT::ScheduledAudit	Oui	Non	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::IoT::SecurityProfile	Oui	Non	Oui	Non
AWS::KMS::Alias	Oui	Oui	Non	Non
AWS::KMS::Key	Oui	Oui	Oui	Oui
AWS::Kinesis::Stream	Oui	Oui	Oui	Non
AWS::Kinesis::StreamConsumer	Oui	Oui	Oui	Non
AWS::KinesisAnalyticsV2::Application	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::KinesisFirehose::DeliveryStream	Oui	Oui	Oui	Oui
AWS::Lambda::CodeSigningConfig	Oui	Oui	Non	Non
AWS::Lambda::Function	Oui	Oui	Oui	Oui
AWS::Lex::Bot	Non	Oui	Non	Non
AWS::Lex::BotAlias	Non	Oui	Non	Non
AWS::Logs::Destination	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::MSK::BatchScramSecret	Oui	Oui	Oui	Non
AWS::MSK::Cluster	Oui	Oui	Oui	Non
AWS::MSK::ClusterPolicy	Oui	Oui	Oui	Oui
AWS::MSK::Configuration	Oui	Oui	Oui	Non
AWS::MSK::VpcConnection	Oui	Oui	Oui	Oui
AWS::MediaConnect::FlowEntitlement	Non	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::MediaConnect::FlowSource	Non	Oui	Non	Non
AWS::MediaConnect::FlowVpcInterface	Non	Oui	Non	Non
AWS::MediaTailor::PlaybackConfiguration	Non	Oui	Non	Non
AWS::NetworkFirewall::Firewall	Oui	Oui	Oui	Oui
AWS::NetworkFirewall::FirewallPolicy	Oui	Oui	Oui	Oui
AWS::NetworkFirewall::RuleGroup	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::NetworkPare-feu : :TLS InspectionConfiguration	Oui	Oui	Oui	Oui
AWS::OpenSearch::Domain	Oui	Oui	Non	Non
AWS::RDS::DBCluster	Oui	Oui	Oui	Non
AWS : :RDS : :DB ClusterSnapshot	Oui	Oui	Oui	Non
AWS::RDS::DBInstance	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SecurityGroup	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::RDS::DBSnapshot	Oui	Oui	Oui	Oui
AWS : :RDS : :DB SubnetGroup	Oui	Oui	Oui	Oui
AWS::RDS::EventSubscription	Oui	Oui	Oui	Oui
AWS::RDS::OptionGroup	Oui	Oui	Oui	Non
AWS::Redshift::Cluster	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterParameterGroupe	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::Redshift::ClusterSecurityGroupe	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSnapshot	Oui	Oui	Oui	Oui
AWS::Redshift::ClusterSubnetGroupe	Oui	Oui	Oui	Oui
AWS::Redshift::EventSubscription	Oui	Oui	Oui	Oui
AWS::Redshift::ScheduledAction	Oui	Non	Non	Non
AWS::ResilienceHub::App	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ResilienceHub::ResiliencyPolicy	Oui	Oui	Non	Non
AWS::Route53Resolver::FirewallDomainListe	Oui	Oui	Non	Non
AWS::Route53Resolver::FirewallRuleGroupe	Oui	Oui	Non	Non
AWS::Route53Resolver::FirewallRuleGroupAssociation	Oui	Oui	Non	Non
AWS::Route53Resolver::ResolverEndpoint	Oui	Oui	Oui	Non
AWS::Route53Resolver::ResolverQueryLoggingConfig	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Oui	Oui	Non	Non
AWS::Route53Resolver::ResolverRule	Oui	Oui	Oui	Non
AWS::Route53Resolver::ResolverRuleAssociation	Oui	Oui	Oui	Non
AWS::S3::AccessPoint	Oui	Oui	Oui	Oui
AWS::S3::AccountPublicAccessBlock	Oui	Oui	Non	Non
AWS::S3::Bucket	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::SES::ConfigurationSet	Oui	Oui	Non	Non
AWS::SES::ContactList	Oui	Oui	Non	Non
AWS::SES::Template	Oui	Oui	Non	Non
AWS::SNS::Topic	Oui	Oui	Non	Non
AWS::SQS::Queue	Oui	Oui	Non	Non
AWS::SSM::AssociationCompliance	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::SSM::Document	Oui	Oui	Oui	Oui
AWS::SSM::FileData	Oui	Oui	Oui	Oui
AWS::SSM::ManagedInstanceInventaire	Oui	Oui	Oui	Oui
AWS::SSM::PatchCompliance	Oui	Oui	Oui	Oui
AWS::SageMaker::AppImageConfig	Oui	Oui	Non	Non
AWS::SageMaker::CodeRepository	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::SageMaker::Domain	Oui	Oui	Non	Non
AWS::SageMaker::EndpointConfig	Oui	Oui	Non	Non
AWS::SageMaker::FeatureGroup	Oui	Oui	Non	Non
AWS::SageMaker::Image	Oui	Oui	Non	Non
AWS::SageMaker::Model	Oui	Oui	Non	Non
AWS::SageMaker::NotebookInstance	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Oui	Oui	Non	Non
AWS::SecretsManager::Secret	Oui	Oui	Oui	Oui
AWS::ServiceCatalog::CloudFormationProduit	Oui	Oui	Oui	Non
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Oui	Oui	Oui	Non
AWS::ServiceCatalog::Portfolio	Oui	Oui	Oui	Non
AWS::ServiceDiscovery::HttpNamespace	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::ServiceDiscovery::Instance	Oui	Oui	Oui	Non
AWS::ServiceDiscovery::PublicDnsEspace de noms	Oui	Oui	Oui	Non
AWS::ServiceDiscovery::Service	Oui	Oui	Oui	Non
AWS::ShieldRegional::Protection	Oui	Oui	Oui	Non
AWS::Signer::SigningProfile	Oui	Oui	Non	Non
AWS::StepFunctions::Activity	Oui	Oui	Oui	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::StepFunctions::StateMachine	Oui	Oui	Oui	Non
AWS::Transfer::Agreement	Oui	Oui	Oui	Non
AWS::Transfer::Certificate	Oui	Oui	Oui	Non
AWS::Transfer::Connector	Oui	Oui	Oui	Non
AWS::Transfer::Profile	Oui	Oui	Oui	Oui
AWS::Transfer::Workflow	Oui	Oui	Non	Non

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::WAFRegional::RateBasedRègle	Oui	Oui	Oui	Oui
AWS::WAFRegional::Rule	Oui	Oui	Oui	Oui
AWS::WAFRegional::RuleGroup	Oui	Oui	Oui	Oui
AWS::WAFRegional::WebACL	Oui	Oui	Oui	Oui
AWS::WAFv2::IPSet	Oui	Oui	Oui	Oui
AWS::WAFv2::ManagedRuleSet	Oui	Oui	Oui	Oui

Type de ressource	Afrique (Le Cap)	Moyen-Orient (Bahreïn)	Moyen-Orient (EAU)	Israël (Tel Aviv)
AWS::WAFv2::RegexPatternSet	Oui	Oui	Oui	Oui
AWS::WAFv2::RuleGroup	Oui	Oui	Oui	Oui
AWS::WAFv2::WebACL	Oui	Oui	Oui	Oui
AWS::WorkSpaces::Workspace	Non	Oui	Non	Non
AWS::XRay::EncryptionConfig	Non	Oui	Oui	Oui

GovCloud Régions

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::ACM::Certificate	Oui	Oui
AWS::ACMPCA::CertificateAuthority	Oui	Oui
AWS::ACMPCA::CertificateAuthorityActivation	Oui	Oui
AWS::AccessAnalyzer::Analyzer	Oui	Oui
AWS::AmazonMQ::Broker	Oui	Oui
AWS::ApiGateway::RestApi	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::ApiGateway::Stage	Oui	Oui
AWS::ApiGatewayV2::Api	Oui	Oui
AWS::ApiGatewayV2::Stage	Oui	Oui
AWS::AppConfig::Application	Oui	Oui
AWS::AppConfig::ConfigurationProfile	Oui	Oui
AWS::AppConfig::DeploymentStrategy	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::AppConfig::Environment	Oui	Oui
AWS::AppConfig::ExtensionAssociation	Oui	Oui
AWS::AppConfig::HostedConfigurationVersion	Oui	Oui
AWS::AppStream::Application	Oui	Oui
AWS::AppStream::DirectoryConfig	Non	Oui
AWS::AppStream::Fleet	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::AppStream::Stack	Non	Oui
AWS::Athena::DataCatalog	Oui	Oui
AWS::Athena::WorkGroup	Oui	Oui
AWS::AutoScaling::AutoScalingGroupe	Oui	Oui
AWS::AutoScaling::LaunchConfiguration	Oui	Oui
AWS::AutoScaling::ScalingPolicy	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::AutoScaling::ScheduledAction	Oui	Oui
AWS::AutoScaling::WarmPool	Oui	Oui
AWS::Backup::BackupPlan	Oui	Oui
AWS::Backup::BackupSelection	Oui	Oui
AWS::Backup::BackupVault	Oui	Oui
AWS::Backup::RecoveryPoint	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Batch::ComputeEnvironment	Oui	Oui
AWS::Batch::JobQueue	Oui	Oui
AWS::Batch::SchedulingPolicy	Oui	Oui
AWS::Cassandra::Keyspace	Oui	Oui
AWS::CloudFormation::Stack	Oui	Oui
AWS::CloudTrail::Trail	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::CloudWatch::Alarm	Oui	Oui
AWS::CodeBuild::Project	Oui	Oui
AWS::CodeBuild::ReportGroup	Oui	Oui
AWS::Cognito::UserPoolGroupe	Non	Oui
AWS::Config::ConfigurationRecorder	Oui	Oui
AWS::Config::ConformancePackConformité	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Config::ResourceCompliance	Oui	Oui
AWS::Connect::Instance	Non	Oui
AWS::Connect::QuickConnect	Non	Oui
AWS::DMS::Certificate	Oui	Oui
AWS::DMS::Endpoint	Oui	Oui
AWS::DMS::EventSubscription	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::DMS::ReplicationInstance	Oui	Oui
AWS::DMS::ReplicationSubnetGroupe	Oui	Oui
AWS::DMS::ReplicationTask	Oui	Oui
AWS::DataSync::LocationEFS	Oui	Oui
AWS::DataSync::LocationF SxLustre	Oui	Oui
AWS::DataSync::LocationF SxWindows	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::DataSync::LocationHDFS	Oui	Oui
AWS::DataSync::LocationNFS	Oui	Oui
AWS::DataSync::LocationObjectRangement	Oui	Oui
AWS::DataSync::LocationS3	Oui	Oui
AWS::DataSync::LocationPME	Oui	Oui
AWS::DataSync::Task	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Detective::Graph	Oui	Oui
AWS::DynamoDB::Table	Oui	Oui
AWS::EC2::CapacityReservation	Oui	Oui
AWS::EC2::ClientVpnPoint final	Oui	Oui
AWS::EC2::CustomerGateway	Oui	Oui
AWS::EC2::DHCPOptions	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::EC2::EC2Fleet	Oui	Oui
AWS::EC2::EIP	Oui	Oui
AWS::EC2::EgressOnlyInternetGateway	Oui	Oui
AWS::EC2::FlowLog	Oui	Oui
AWS::EC2::Host	Oui	Oui
AWS::EC2::IPAM	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::EC2::IPAMPool	Oui	Oui
AWS::EC2::IPAMScope	Oui	Oui
AWS::EC2::Instance	Oui	Oui
AWS::EC2::InternetGateway	Oui	Oui
AWS::EC2::LaunchTemplate	Oui	Oui
AWS::EC2::NatGateway	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::EC2::NetworkAcl	Oui	Oui
AWS::EC2::NetworkInterface	Oui	Oui
AWS::EC2::PrefixList	Oui	Oui
AWS::EC2::RouteTable	Oui	Oui
AWS::EC2::SecurityGroup	Oui	Oui
AWS::EC2::SpotFleet	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::EC2::Subnet	Oui	Oui
AWS::EC2::SubnetRouteTableAssociation	Oui	Oui
AWS::EC2::TrafficMirrorFiltre	Oui	Oui
AWS::EC2::TrafficMirrorSéance	Oui	Oui
AWS::EC2::TrafficMirrorCible	Oui	Oui
AWS::EC2::TransitGateway	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::EC2::TransitGatewayPièce jointe	Oui	Oui
AWS::EC2::TransitGatewayConnect	Oui	Oui
AWS::EC2::TransitGatewayMulticastDomain	Oui	Oui
AWS::EC2::TransitGatewayRouteTable	Oui	Oui
AWS::EC2::VPC	Oui	Oui
AWS::EC2::VPCEndpoint	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS : :EC2 : :VPC EndpointService	Non	Oui
AWS : :EC2 : :VPC PeeringConnection	Oui	Oui
AWS::EC2::VPNConnection	Oui	Oui
AWS::EC2::VPNGateway	Oui	Oui
AWS::EC2::Volume	Oui	Oui
AWS::ECR::Repository	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::ECS::CapacityProvider	Oui	Oui
AWS::ECS::Cluster	Oui	Oui
AWS::ECS::Service	Oui	Oui
AWS::ECS::TaskDefinition	Oui	Oui
AWS::ECS::TaskSet	Oui	Oui
AWS::EFS::AccessPoint	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::EFS::FileSystem	Oui	Oui
AWS::EKS::Addon	Oui	Oui
AWS::EKS::Cluster	Oui	Oui
AWS::EKS::IdentityProviderConfig	Oui	Oui
AWS::EMR::SecurityConfiguration	Oui	Oui
AWS::ElasticBeanstalk::Application	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::ElasticBeanstalk::ApplicationVersion	Oui	Oui
AWS::ElasticBeanstalk::Environment	Oui	Oui
AWS::ElasticLoadBalancing::LoadBalancer	Oui	Oui
AWS::ElasticLoadBalancingV2::Listener	Oui	Oui
AWS::ElasticLoadBalancingV2::LoadBalancer	Oui	Oui
AWS::Elasticsearch::Domain	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Events::EventBus	Oui	Oui
AWS::Events::Rule	Oui	Oui
AWS::FIS::ExperimentTemplate	Oui	Oui
AWS::Glue::Classifier	Oui	Oui
AWS::Glue::Job	Oui	Oui
AWS::Glue::MLTransform	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::GreengrassV2::ComponentVersion	Oui	Oui
AWS::GuardDuty::Detector	Oui	Oui
AWS::GuardDuty::Filter	Oui	Oui
AWS::GuardDevoir : IPset	Oui	Oui
AWS::GuardDuty::ThreatIntelSet	Oui	Oui
AWS::IAM::Group	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::IAM::InstanceProfile	Oui	Non
AWS::IAM::OIDCProvider	Oui	Non
AWS::IAM::Policy	Oui	Oui
AWS::IAM::Role	Oui	Oui
AWS::IAM::SAMLProvider	Oui	Non
AWS::IAM::ServerCertificate	Oui	Non

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::IAM::User	Oui	Oui
AWS::ImageBuilder::ContainerRecipe	Oui	Oui
AWS::ImageBuilder::DistributionConfiguration	Oui	Oui
AWS::ImageBuilder::ImagePipeline	Oui	Oui
AWS::ImageBuilder::ImageRecipe	Oui	Oui
AWS::ImageBuilder::InfrastructureConfiguration	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::IoT::AccountAuditConfiguration	Oui	Oui
AWS::IoT::Authorizer	Oui	Oui
AWS::IoCertificat T : :CA	Oui	Oui
AWS::IoT::CustomMetric	Oui	Oui
AWS::IoT::Dimension	Oui	Oui
AWS::IoT::FleetMetric	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::IoT::JobTemplate	Oui	Oui
AWS::IoT::MitigationAction	Oui	Oui
AWS::IoT::Policy	Oui	Oui
AWS::IoT::ProvisioningTemplate	Oui	Oui
AWS::IoT::RoleAlias	Oui	Oui
AWS::IoT::ScheduledAudit	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::IoT::SecurityProfile	Oui	Oui
AWS::IoTEvents::AlarmModel	Non	Oui
AWS::IoTEvents::DetectorModel	Non	Oui
AWS::IoTEvents::Input	Non	Oui
AWS::IoTSiteWise::AssetModel	Non	Oui
AWS::IoTSiteWise::Gateway	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::IoTSiteWise::Portal	Non	Oui
AWS::IoTTwinMaker::ComponentType	Non	Oui
AWS::IoTTwinMaker::Entity	Non	Oui
AWS::IoTTwinMaker::Workspace	Non	Oui
AWS::KMS::Alias	Oui	Oui
AWS::KMS::Key	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Kinesis::Stream	Oui	Oui
AWS::Kinesis::StreamConsumer	Oui	Oui
AWS::KinesisAnalyticsV2::Application	Oui	Oui
AWS::KinesisFirehose::DeliveryStream	Oui	Oui
AWS::Lambda::Function	Oui	Oui
AWS::Logs::Destination	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::MSK::BatchScramSecret	Oui	Oui
AWS::MSK::Cluster	Oui	Oui
AWS::MSK::ClusterPolicy	Oui	Oui
AWS::MSK::Configuration	Oui	Oui
AWS::MSK::VpcConnection	Oui	Oui
AWS::NetworkFirewall::Firewall	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::NetworkFirewall::FirewallPolicy	Oui	Oui
AWS::NetworkFirewall::RuleGroup	Oui	Oui
AWS::NetworkManager::CustomerGatewayAssociation	Non	Oui
AWS::NetworkManager::Device	Non	Oui
AWS::NetworkManager::GlobalNetwork	Non	Oui
AWS::NetworkManager::Link	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::NetworkManager::LinkAssociation	Non	Oui
AWS::NetworkManager::Site	Non	Oui
AWS::NetworkManager::TransitGatewayInscription	Non	Oui
AWS::OpenSearch::Domain	Oui	Oui
AWS::Pinpoint::App	Non	Oui
AWS::Pinpoint::ApplicationSettings	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Pinpoint::Campaign	Non	Oui
AWS::Pinpoint::EmailChannel	Non	Oui
AWS::Pinpoint::EmailTemplate	Non	Oui
AWS::Pinpoint::EventStream	Non	Oui
AWS::Pinpoint::InAppModèle	Non	Oui
AWS::Pinpoint::Segment	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::QuickSight::Template	Non	Oui
AWS::RDS::DBCluster	Oui	Oui
AWS : :RDS : :DB ClusterSnapshot	Oui	Oui
AWS::RDS::DBInstance	Oui	Oui
AWS : :RDS : :DB SecurityGroup	Oui	Oui
AWS::RDS::DBSnapshot	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS : :RDS : :DB SubnetGroup	Oui	Oui
AWS::RDS::EventSubscription	Oui	Oui
AWS::RDS::OptionGroup	Oui	Oui
AWS::Redshift::Cluster	Oui	Oui
AWS::Redshift::ClusterParameterGroupe	Oui	Oui
AWS::Redshift::ClusterSecurityGroupe	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Redshift::ClusterSnapshot	Oui	Oui
AWS::Redshift::ClusterSubnetGroupe	Oui	Oui
AWS::Redshift::EventSubscription	Oui	Oui
AWS::Redshift::ScheduledAction	Oui	Oui
AWS::RoboMaker::RobotApplication	Non	Oui
AWS::RoboMaker::RobotApplicationVersion	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::RoboMaker::SimulationApplication	Non	Oui
AWS::Route53Resolver::FirewallDomainListe	Oui	Oui
AWS::Route53Resolver::FirewallRuleGroupe	Oui	Oui
AWS::Route53Resolver::FirewallRuleGroupAssociation	Oui	Oui
AWS::Route53Resolver::ResolverEndpoint	Oui	Oui
AWS::Route53Resolver::ResolverQueryLoggingConfig	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	Oui	Oui
AWS::Route53Resolver::ResolverRule	Oui	Oui
AWS::Route53Resolver::ResolverRuleAssociation	Oui	Oui
AWS::S3::AccessPoint	Oui	Oui
AWS::S3::AccountPublicAccessBlock	Oui	Oui
AWS::S3::Bucket	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::SES::ConfigurationSet	Non	Oui
AWS::SES::ContactList	Non	Oui
AWS::SES::Template	Non	Oui
AWS::SNS::Topic	Oui	Oui
AWS::SQS::Queue	Oui	Oui
AWS::SSM::AssociationCompliance	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::SSM::Document	Oui	Oui
AWS::SSM::FileData	Oui	Oui
AWS::SSM::ManagedInstanceInventaire	Oui	Oui
AWS::SSM::PatchCompliance	Oui	Oui
AWS::SageMaker::Model	Non	Oui
AWS::SageMaker::NotebookInstance	Non	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Non	Oui
AWS::SecretsManager::Secret	Oui	Oui
AWS::ServiceCatalog::CloudFormationProduit	Oui	Oui
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Oui	Oui
AWS::ServiceCatalog::Portfolio	Oui	Oui
AWS::ServiceDiscovery::HttpNamespace	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::ServiceDiscovery::Instance	Oui	Oui
AWS::ServiceDiscovery::Service	Oui	Oui
AWS::StepFunctions::StateMachine	Oui	Oui
AWS::Transfer::Agreement	Oui	Oui
AWS::Transfer::Certificate	Oui	Oui
AWS::Transfer::Connector	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::Transfer::Profile	Oui	Oui
AWS::Transfer::Workflow	Oui	Oui
AWS::WAFRegional::RateBasedRègle	Oui	Oui
AWS::WAFRegional::Rule	Oui	Oui
AWS::WAFRegional::RuleGroup	Oui	Oui
AWS::WAFRegional::WebACL	Oui	Oui

Type de ressource	AWS GovCloud (US-Ouest)	AWS GovCloud (USA Est)
AWS::WAFv2::IPSet	Oui	Oui
AWS::WAFv2::ManagedRuleSet	Oui	Oui
AWS::WAFv2::RegexPatternSet	Oui	Oui
AWS::WAFv2::RuleGroup	Oui	Oui
AWS::WAFv2::WebACL	Oui	Oui
AWS::WorkSpaces::Workspace	Non	Oui

AWS Ressources d'enregistrement

AWS Config détecte en permanence la création, la modification ou la suppression des types de ressources pris en charge. AWS Config enregistre ces événements en tant qu'éléments de configuration (CI). Vous pouvez personnaliser AWS Config pour enregistrer les changements de configuration de tous les types de ressources pris en charge ou uniquement des types de ressources pris en charge que vous jugez pertinents. Pour obtenir la liste des types de ressources pris en charge qui AWS Config peuvent enregistrer, consultezTypes de ressource pris en charge.

Considérations

Nombre élevé d' AWS Config évaluations

Vous remarquerez peut-être une augmentation de l'activité de votre compte lors de votre premier mois d'enregistrement avec AWS Config par rapport aux mois suivants. Au cours du processus de démarrage initial, AWS Config exécute des évaluations sur toutes les ressources de votre compte que vous avez sélectionnées AWS Config pour enregistrement.

Si vous exécutez des charges de travail éphémères, vous constaterez peut-être une augmentation de l'activité en raison de AWS Config l'enregistrement des modifications de configuration associées à la création et à la suppression de ces ressources temporaires. Une charge de travail éphémère est une utilisation temporaire des ressources informatiques chargées et exécutées si nécessaire. Il peut par exemple s'agir des instances Spot Amazon Elastic Compute Cloud (Amazon EC2), des tâches Amazon EMR et d' AWS Auto Scaling. Si vous souhaitez éviter l'augmentation de l'activité liée à l'exécution de charges de travail éphémères, vous pouvez configurer l'enregistreur de configuration pour exclure l'enregistrement de ces types de ressources, ou exécuter ces types de charges de travail dans un compte distinct en désactivant pour éviter d' AWS Config augmenter l'enregistrement des configurations et l'évaluation des règles.

Disponibilité dans les Régions

Avant de spécifier un type de ressource AWS Config à suivre, vérifiez la disponibilité des ressources par région pour voir si le type de ressource est pris en charge dans la AWS région où vous l'avez configuré AWS Config. Si un type de ressource est pris AWS Config en charge par au moins une région, vous pouvez activer l'enregistrement de ce type de ressource dans toutes les régions prises en charge AWS Config, même si le type de ressource spécifié n'est pas pris en charge dans la AWS région où vous l'avez configuré AWS Config.

Quelles sont les différences entre les ressources régionales et mondiales ?

Ressources régionales

Les ressources régionales sont liées à une région et peuvent être utilisées uniquement dans celle-ci. Vous les créez dans une région spécifiée Région AWS, puis ils existent dans cette région. Pour voir ou interagir avec ces ressources, vous devez diriger vos opérations vers cette région. Par exemple, pour créer une instance Amazon EC2 avec AWS Management Console, vous devez choisir Région AWS celle dans laquelle vous souhaitez créer l'instance. Si vous utilisez le AWS Command Line Interface (AWS CLI) pour créer l'instance, vous incluez le `--region` paramètre. Les AWS SDK ont chacun leur propre mécanisme équivalent pour spécifier la région utilisée par l'opération.

Plusieurs raisons justifient l'utilisation des ressources régionales. L'une des raisons vise à garantir que les ressources et les points de terminaison de service que vous utilisez pour y accéder soient aussi proches que possible du client. Les performances sont ainsi améliorées grâce à la réduction de la latence. Une autre raison vise à fournir une limite d'isolement. Vous pouvez ainsi créer des copies indépendantes des ressources dans plusieurs régions afin de répartir la charge et d'améliorer la capacité de mise à l'échelle. Par ailleurs, les ressources sont isolées les unes des autres afin d'améliorer leur disponibilité.

Si vous en spécifiez une autre Région AWS dans la console ou dans une AWS CLI commande, vous ne pouvez plus voir ou interagir avec les ressources que vous pouviez voir dans la région précédente.

Lorsque vous examinez l'Amazon Resource Name (ARN) d'une ressource régionale, la région qui contient la ressource est spécifiée dans le quatrième champ de l'ARN. Par exemple, une instance Amazon EC2 est une ressource régionale. Voici un exemple d'un ARN pour une instance Amazon EC2 disponible dans la région `us-east-1`.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Ressources globales

Certaines ressources de AWS services sont des ressources globales, ce qui signifie que vous pouvez utiliser la ressource de n'importe où. Aucune Région AWS ne doit être spécifiée dans la console d'un service global. Pour accéder à une ressource globale, vous ne devez pas spécifier de `--region` paramètre lorsque vous utilisez les opérations du service AWS CLI et du AWS SDK.

Les ressources globales prennent en charge les cas où il est essentiel qu'une seule instance d'une ressource particulière puisse exister à la fois. Dans ces scénarios, la réplication ou la synchronisation entre des copies situées dans différentes régions ne sont pas adéquates. L'accès à un point de terminaison global unique, associé à une augmentation éventuelle de la latence, est considéré comme acceptable pour garantir que tout changement soit instantanément visible pour les consommateurs de la ressource.

Par exemple, les clusters globaux Amazon Aurora (`AWS::RDS::GlobalCluster`) sont des ressources globales et ne sont donc pas liés à une région. Vous pouvez donc créer un cluster global sans dépendre d'un point de terminaison régional. Cette démarche offre un avantage : même si Amazon Relational Database Service (Amazon RDS) est organisé par régions, la région spécifique d'où provient un cluster global n'a aucune incidence sur ce dernier. Il apparaît comme un cluster global unique et continu dans toutes les régions.

L'Amazon Resource Name (ARN) d'une ressource globale n'inclut pas de région. Le quatrième champ est vide, comme dans l'exemple suivant de l'ARN d'un cluster global.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> Les types de ressources globales intégrés AWS Config après février 2022 ne seront enregistrés que dans la région d'origine du service pour la partition commerciale et AWS GovCloud (USA Ouest) pour la partition. GovCloud Vous pouvez consulter les éléments de configuration (CI) de ces nouveaux types de ressources globales uniquement dans leur région d'origine et AWS GovCloud (USA Ouest).
> Les types de ressources mondiales intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role` et`AWS::IAM::User`) restent inchangés. Vous pouvez activer l'enregistrement de ces ressources IAM mondiales dans toutes les régions où elles AWS Config étaient prises en charge avant février 2022. Ces ressources IAM mondiales ne peuvent pas être enregistrées dans les régions prises en charge AWS Config après février 2022.

Types de ressources mondiales | Ressources IAM

Les types de ressources IAM suivants sont également enregistrés au niveau mondial : utilisateurs, groupes et rôles IAM, et politiques gérées par le client. Ces types de ressources

peuvent être enregistrés AWS Config dans les régions où AWS Config ils étaient disponibles avant février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Pour éviter la duplication des éléments de configuration (CI), vous devez envisager de n'enregistrer les types de ressources IAM globaux qu'une seule fois dans l'une des régions prises en charge. Cela peut également vous aider à éviter les évaluations inutiles et la limitation des API.

Types de ressources mondiales | Région d'origine uniquement

Les ressources globales pour les services suivants sont uniquement enregistrées AWS Config dans la région d'origine du type de ressource globale : Amazon Elastic Container Registry Public AWS Global Accelerator, Amazon Route 53 CloudFront, Amazon et AWS WAF. Pour ces ressources globales, la même instance du type de ressource peut être utilisée dans plusieurs AWS régions, mais les éléments de configuration (CI) ne sont enregistrés que dans la région d'origine pour la partition commerciale ou AWS GovCloud (US-West) pour la AWS GovCloud (US) partition.

Régions d'origine des types de ressources globales

AWS Service	Valeur de type de ressource	Région d'accueil
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	Région USA Est (Virginie du Nord)
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	Région USA Ouest (Oregon)
	`AWS::GlobalAccelerator::EndpointGroup`	Région USA Ouest (Oregon)
	`AWS::GlobalAccelerator::Accelerator`	Région USA Ouest (Oregon)
Amazon Route 53	`AWS::Route53::HostedZone`	Région USA Est (Virginie du Nord)

AWS Service	Valeur de type de ressource	Région d'accueil
	`AWS::Route53::HealthCheck`	Région USA Est (Virginie du Nord)
Amazon CloudFront	`AWS::CloudFront::Distribution`	Région USA Est (Virginie du Nord)
AWS WAF	`AWS::WAFv2::WebACL`	Région USA Est (Virginie du Nord)

Types de ressources mondiales | Clusters Aurora mondiaux

`AWS::RDS::GlobalCluster`est une ressource globale enregistrée dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé. Ce type de ressource globale est unique en ce sens que si vous activez l'enregistrement de cette ressource dans une région, vous AWS Config enregistrerez les éléments de configuration (CI) pour ce type de ressource dans toutes vos régions activées.

Si vous ne souhaitez pas enregistrer `AWS::RDS::GlobalCluster` dans toutes les régions activées, appliquez l'une des stratégies d'enregistrement suivantes pour la AWS Config console :

- Enregistrez tous les types de ressources avec des remplacements personnalisables, choisissez « AWS RDS », GlobalCluster puis choisissez le remplacement « Exclure de l'enregistrement »
- Enregistrer des types de ressources spécifiques.

Si vous ne souhaitez pas enregistrer `AWS::RDS::GlobalCluster` dans toutes les régions activées, utilisez l’une des politiques d’enregistrement suivantes pour l’API/l’interface de ligne de commande :

- Enregistrer tous les types de ressources actuels et futurs avec des exclusions (`EXCLUSION_BY_RESOURCE_TYPES`)
- Enregistrer des types de ressources spécifiques (`INCLUSION_BY_RESOURCE_TYPES`).

Ressources d'enregistrement dans la AWS Config console

Enregistrement de ressources (console)

Vous pouvez utiliser la AWS Config console pour sélectionner les types de ressources qui AWS Config enregistrent.

Pour sélectionner des ressources

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le volet de navigation de gauche, choisissez Agir puis Règles. Pour obtenir la liste des régions prises en charge, consultez Points de terminaison et quotas AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans la section Méthode d'enregistrement, choisissez une stratégie d'enregistrement. Vous pouvez spécifier les AWS ressources que vous AWS Config souhaitez enregistrer.

   All resource types with customizable overrides

   Configuré AWS Config pour enregistrer les modifications de configuration pour tous les types de ressources pris en charge actuels et futurs dans cette région. Vous pouvez modifier la fréquence d'enregistrement de types de ressources spécifiques ou exclure certains types de ressources de l'enregistrement. Pour plus d'informations, consultez Types de ressources pris en charge.

   - Paramètres par défaut

     Configurez la fréquence d'enregistrement par défaut de tous les types de ressources actuels et futurs pris en charge. Pour plus d'informations, consultez Fréquence d'enregistrement.

     - Enregistrement continu : AWS Config enregistre les modifications de configuration en continu chaque fois qu'une modification se produit.
     - Enregistrement quotidien : vous recevrez un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il est différent de l'élément de configuration enregistré précédemment.

> **Note**
>
> AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

- Paramètres de remplacement

  Modifiez la fréquence d'enregistrement de types de ressources spécifiques ou excluez des types de ressources spécifiques de l'enregistrement. Si vous modifiez la fréquence d'enregistrement d'un type de ressource ou si vous arrêtez l'enregistrement d'un type de ressource, les éléments de configuration déjà enregistrés resteront inchangés.

> **Note**
>
> Types de ressources mondiales | Les clusters Aurora mondiaux sont initialement inclus dans l'enregistrement
> Le type de `AWS::RDS::GlobalCluster` ressource sera enregistré dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé.
> Si vous ne souhaitez pas enregistrer `AWS::RDS::GlobalCluster` dans toutes les régions activées, choisissez « AWS RDS GlobalCluster », puis choisissez l'option « Exclure de l'enregistrement ».

> **Note**
>
> Types de ressources mondiales | Les types de ressources IAM sont initialement exclus de l'enregistrement
> « Tous les types de ressources IAM enregistrés au niveau mondial » sont initialement exclus de l'enregistrement pour vous aider à réduire vos coûts. Cela inclut les utilisateurs, les groupes et les rôles IAM, ainsi que les politiques gérées par le client. Choisissez Supprimer pour supprimer l'exclusion et inclure ces ressources dans votre enregistrement.
> L'exception à cette note concerne la région USA Est (Virginie du Nord). Les types de ressources IAM enregistrés au niveau mondial sont initialement inclus dans la

région USA Est (Virginie du Nord), car cette région fonctionne comme la région d'origine des types de ressources IAM mondiales.
En outre, les types de ressources IAM globaux (`AWS::IAM::User`, `AWS::IAM::GroupAWS::IAM::Role`, et`AWS::IAM::Policy`) ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

> **Note**
>
> Restrictions
>
> Vous pouvez ajouter jusqu'à 100 exclusions de fréquence et 600 exclusions d'exclusion.
>
> L'enregistrement quotidien ne prend pas en charge les types de ressources suivants :
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Specific resource types

Configurez AWS Config pour enregistrer les modifications de configuration uniquement pour les types de ressources que vous spécifiez.

- Types de ressources spécifiques

  Choisissez un type de ressource à enregistrer et sa fréquence. Pour plus d'informations, consultez Fréquence d'enregistrement.

  - Enregistrement continu : AWS Config enregistre les modifications de configuration en continu chaque fois qu'une modification se produit.
  - Enregistrement quotidien : vous recevrez un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il est différent de l'élément de configuration enregistré précédemment.

> **Note**
>
> AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

Si vous modifiez la fréquence d'enregistrement d'un type de ressource ou si vous arrêtez l'enregistrement d'un type de ressource, les éléments de configuration déjà enregistrés resteront inchangés.

> **Note**
>
> Disponibilité dans les Régions
> Avant de spécifier un type de ressource AWS Config à suivre, vérifiez la disponibilité des ressources par région pour voir si le type de ressource est pris en charge dans la AWS région où vous l'avez configuré AWS Config. Si un type de ressource est pris AWS Config en charge par au moins une région, vous pouvez activer l'enregistrement de ce type de ressource dans toutes les régions prises en charge AWS Config, même si le type de ressource spécifié n'est pas pris en charge dans la AWS région où vous l'avez configuré AWS Config.

> **Note**
>
> Restrictions
> Aucune limite si tous les types de ressources ont la même fréquence. Vous pouvez ajouter jusqu'à 100 types de ressources avec une fréquence quotidienne si au moins un type de ressource est défini sur Continu.
> La fréquence quotidienne n'est pas prise en charge pour les types de ressources suivants :
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

4. Choisissez Save pour enregistrer les changements.

Enregistrer des ressources avec la AWS CLI

Ressources d'enregistrement (AWS CLI)

Vous pouvez utiliser la AWS CLI pour sélectionner les types de ressources que vous AWS Config souhaitez enregistrer. Pour cela, créez un enregistreur de configuration, qui enregistre les types de ressources que vous spécifiez dans un groupe d'enregistrement. Dans le groupe d'enregistrement, vous spécifiez si vous souhaitez enregistrer tous les types de ressources pris en charge ou si vous souhaitez inclure ou exclure des types de ressources spécifiques.

Record all current and future supported resource types

Configuré AWS Config pour enregistrer les modifications de configuration pour tous les types de ressources pris en charge actuels et futurs dans cette région. Pour plus d'informations, consultez Types de ressources pris en charge.

1. Utilisez la commande `put-configuration-recorder` suivante :

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Cette commande utilise les `---recording-group` champs `--configuration-recorder` et.

> **Note**
>
> Groupe d'enregistrement et enregistreur de configuration
> Le champ `--recording-group` indique les types de ressources enregistrés.
> Le `--configuration-recorder` champ indique `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

i. `put-configuration-recorder` utilise les champs suivants pour le paramètre `--recording-group` :

- `allSupported=true`— AWS Config enregistre les modifications de configuration pour tous les types de ressources pris en charge, à l'exception des types de ressources IAM globaux. Lorsque AWS Config la prise en charge d'un nouveau type de ressource est ajoutée, AWS Config commence à enregistrer automatiquement les ressources de ce type.
- `includeGlobalResourceTypes=true` : cette option concerne uniquement les types de ressource IAM mondiales : utilisateurs, groupes et rôles IAM, et politiques gérées par le client. Ces types de ressources IAM globaux ne peuvent être enregistrés que AWS Config dans les régions où ils AWS Config étaient disponibles avant février 2022. Vous ne pouvez pas enregistrer les types de ressources IAM globaux dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

> **Important**
>
> Les clusters globaux Aurora sont enregistrés dans toutes les régions activées
> Le type de `AWS::RDS::GlobalCluster` ressource sera enregistré dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé, même s'il n'`includeGlobalResourceTypes`est pas défini sur`true`.
> L'option `includeGlobalResourceTypes` s'applique uniquement aux utilisateurs, aux groupes et aux rôles IAM, ainsi qu'aux politiques gérées par le client.
> Si vous ne souhaitez pas enregistrer `AWS::RDS::GlobalCluster` dans toutes les régions activées, utilisez l'une des politiques d'enregistrement suivantes :
>
> 1. Enregistrer tous les types de ressources actuels et futurs, à l'exception des types que vous spécifiez (`EXCLUSION_BY_RESOURCE_TYPES`), ou
> 2. Enregistrer des types de ressources spécifiques (`INCLUSION_BY_RESOURCE_TYPES`).
>
> Pour plus d'informations, consultez Sélection des ressources qui sont enregistrées | Ressources régionales et mondiales.

> **Important**
>
> inclusion GlobalResourceTypes et stratégie d'enregistrement des exclusions
> Le `includeGlobalResourceTypes` champ n'a aucun impact sur la stratégie `EXCLUSION_BY_RESOURCE_TYPES` d'enregistrement. Cela signifie que les types de ressources IAM globaux (utilisateurs IAM, groupes, rôles et politiques gérées par le client) ne seront pas automatiquement ajoutés en tant qu'exclusions pour le `exclusionByResourceTypes` moment `includeGlobalResourceTypes` défini sur. `false`
> Le `includeGlobalResourceTypes` champ ne doit être utilisé que pour modifier le `AllSupported` champ, car le champ par défaut est d'enregistrer les `AllSupported` modifications de configuration pour tous les types de ressources pris en charge, à l'exception des types de ressources IAM globaux.
> Pour inclure les types de ressources IAM globaux lorsqu'il `AllSupported` est défini sur`true`, assurez-vous de `includeGlobalResourceTypes` définir `true` sur.
> Pour exclure les types de ressources IAM globaux pour la stratégie `EXCLUSION_BY_RESOURCE_TYPES` d'enregistrement, vous devez les ajouter manuellement `resourceTypes` dans le champ de`exclusionByResourceTypes`.

> **Note**
>
> Champs obligatoires et facultatifs
> Avant de définir `includeGlobalResourceTypes` sur `true`, définissez le champ `allSupported` sur `true`.
> Vous pouvez éventuellement définir le champ `useOnly` de `RecordingStrategy` sur `ALL_SUPPORTED_RESOURCE_TYPES` (facultatif).

> **Note**
>
> Champs de remplacement

Si vous définissez cette `includeGlobalResourceTypes` option`false`, mais que vous listez les types de ressources IAM globaux dans le `resourceTypes` champ de RecordingGroup, les modifications de configuration pour les types de ressources spécifiés AWS Config seront toujours enregistrées, que vous ayez défini le `includeGlobalResourceTypes` champ sur false ou non.
Si vous ne souhaitez pas enregistrer les changements de configuration apportés aux types de ressources IAM enregistrés au niveau mondial (utilisateurs, groupes et rôles IAM, ainsi que les politiques gérées par le client), veillez à ne pas les répertorier dans le champ `resourceTypes` si le champ `includeGlobalResourceTypes` est défini sur false.

Le fichier `recordingGroup.json` spécifie les types de ressources qui seront enregistrés par AWS Config .

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

ii. `put-configuration-recorder` utilise les champs suivants pour le paramètre `--configuration-recorder` :

- `name`— Nom de l'enregistreur de configuration. AWS Config attribue automatiquement le nom « par défaut » lors de la création de l'enregistreur de configuration.
- `roleARN`— Amazon Resource Name (ARN) du rôle IAM assumé AWS Config et utilisé par l'enregistreur de configuration.
- `recordingMode`— Spécifie la fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration. AWS Config prend en charge l'enregistrement continu et l'enregistrement quotidien. L'enregistrement en continu vous permet d'enregistrer les modifications de configuration en continu, chaque fois qu'un changement a lieu. L'enregistrement quotidien vous permet de recevoir un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il diffère de l'élément de configuration enregistré précédemment.

- `recordingFrequency`— Fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration.

> **Note**
>
> AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

- `recordingModeOverrides` : ce champ vous permet de définir vos exclusions pour le mode d'enregistrement. Il s'agit d'un tableau d'objets `recordingModeOverride`. Chaque objet `recordingModeOverride` du tableau `recordingModeOverrides` comprend trois champs :
  - `description` : description que vous fournissez pour l'exclusion.
  - `recordingFrequency` : fréquence d'enregistrement qui sera appliquée à tous les types de ressources spécifiés dans l'exclusion.
  - `resourceTypes`— Liste séparée par des virgules qui indique les types de ressources AWS Config inclus dans la dérogation.

> **Note**
>
> Champs obligatoires et facultatifs
>
> Le champ `recordingMode` pour `put-configuration-recorder` est facultatif. Par défaut, la fréquence d'enregistrement de l'enregistreur de configuration est définie sur Enregistrement en continu.

> **Note**
>
> Restrictions
>
> L'enregistrement quotidien ne prend pas en charge les types de ressources suivants :
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Pour la stratégie d'enregistrement Enregistrer tous les types de ressources actuels et futurs pris en charge (`ALL_SUPPORTED_RESOURCE_TYPES`), ces types de ressources seront définis sur Enregistrement en continu.

Le `configurationRecorder.json` fichier spécifie `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Facultatif) Pour vérifier que votre enregistreur de configuration présente les paramètres souhaités, utilisez la commande `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

Voici un exemple de réponse.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
```

```
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

Configurez AWS Config pour enregistrer les modifications de configuration pour tous les types de ressources pris en charge actuels et futurs, y compris les types de ressources globaux, à l'exception des types de ressources que vous spécifiez pour exclure de l'enregistrement. Si vous choisissez d'arrêter l'enregistrement pour un type de ressource, les éléments de configuration déjà enregistrés resteront inchangés. Pour plus d'informations, consultez Types de ressources pris en charge.

Cette commande utilise les `---recording-group` champs `--configuration-recorder` et.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> Groupe d'enregistrement et enregistreur de configuration

Le champ `--recording-group` indique les types de ressources enregistrés. Le `--configuration-recorder` champ indique `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

1. Utilisez la commande `put-configuration-recorder` et spécifiez un ou plusieurs types de ressources à exclure dans le champ `resourceTypes` de `exclusionByResourceTypes`, comme indiqué dans l'exemple suivant.

   i. Le fichier `recordingGroup.json` spécifie les types de ressources qui seront enregistrés par AWS Config .

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

   Avant de pouvoir spécifier les types de ressources à exclure de l'enregistrement :

   - Vous devez définir les champs `allSupported` et `includeGlobalResourceTypes` du paramètre `--recording-group` sur `false` ou les omettre.
   - Vous devez définir le champ `useOnly` de `RecordingStrategy` sur `EXCLUSION_BY_RESOURCE_TYPES`.

   > **Note**
   >
   > Champs de remplacement

Si vous choisissez `EXCLUSION_BY_RESOURCE_TYPES` pour la politique d'enregistrement, le champ `exclusionByResourceTypes` remplacera les autres propriétés de la requête.
Par exemple, même si vous définissez `includeGlobalResourceTypes` sur false, les types de ressources IAM mondiales seront toujours enregistrés automatiquement dans cette option, sauf s'ils sont spécifiquement répertoriés en tant qu'exclusions dans le champ `resourceTypes` de `exclusionByResourceTypes`.

> **Note**
>
> Types de ressources globales et politique d'enregistrement des exclusions de ressources
> Par défaut, si vous choisissez la stratégie `EXCLUSION_BY_RESOURCE_TYPES` d'enregistrement, when AWS Config ajoute la prise en charge d'un nouveau type de ressource dans la région où vous avez configuré l'enregistreur de configuration, y compris les types de ressources globaux, AWS Config commence à enregistrer automatiquement les ressources de ce type.
> Sauf mention contraire dans la liste des exclusions, ils `AWS::RDS::GlobalCluster` seront enregistrés automatiquement dans toutes les AWS Config régions prises en charge où l'enregistreur de configuration est activé.
> Les utilisateurs, les groupes, les rôles et les politiques gérées par le client IAM seront enregistrés dans la région dans laquelle vous avez configuré l'enregistreur de configuration s'il s'agit d'une région disponible avant février 2022. AWS Config Vous ne pouvez pas enregistrer les types de ressources IAM globaux dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

ii. `put-configuration-recorder` utilise les champs suivants pour le paramètre `--configuration-recorder` :

- `name`— Nom de l'enregistreur de configuration. AWS Config attribue automatiquement le nom « par défaut » lors de la création de l'enregistreur de configuration.
- `roleARN`— Amazon Resource Name (ARN) du rôle IAM assumé AWS Config et utilisé par l'enregistreur de configuration.
- `recordingMode`— Spécifie la fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration. AWS Config prend en charge

l'enregistrement continu et l'enregistrement quotidien. L'enregistrement en continu vous permet d'enregistrer les modifications de configuration en continu, chaque fois qu'un changement a lieu. L'enregistrement quotidien vous permet de recevoir un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il diffère de l'élément de configuration enregistré précédemment.

- `recordingFrequency`— Fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration.

> **Note**
>
> AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

- `recordingModeOverrides` : ce champ vous permet de définir vos exclusions pour le mode d'enregistrement. Il s'agit d'un tableau d'objets `recordingModeOverride`. Chaque objet `recordingModeOverride` du tableau `recordingModeOverrides` comprend trois champs :
  - `description` : description que vous fournissez pour l'exclusion.
  - `recordingFrequency` : fréquence d'enregistrement qui sera appliquée à tous les types de ressources spécifiés dans l'exclusion.
  - `resourceTypes`— Liste séparée par des virgules qui indique les types de ressources AWS Config inclus dans la dérogation.

> **Note**
>
> Champs obligatoires et facultatifs
> Le champ `recordingMode` pour `put-configuration-recorder` est facultatif. Par défaut, la fréquence d'enregistrement de l'enregistreur de configuration est définie sur Enregistrement en continu.

> **Note**
>
> Restrictions

L'enregistrement quotidien ne prend pas en charge les types de ressources suivants :

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Pour la stratégie d'enregistrement Enregistrer tous les types de ressources actuels et futurs pris en charge (`ALL_SUPPORTED_RESOURCE_TYPES`), ces types de ressources seront définis sur Enregistrement en continu.

Le `configurationRecorder.json` fichier spécifie `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Facultatif) Pour vérifier que votre enregistreur de configuration présente les paramètres souhaités, utilisez la commande `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

Voici un exemple de réponse.

```
{
```

```
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Configurez AWS Config pour enregistrer les modifications de configuration uniquement pour les types de ressources que vous spécifiez. Si vous choisissez d'arrêter l'enregistrement pour un type de ressource, les éléments de configuration déjà enregistrés resteront inchangés.

Cette commande utilise les `---recording-group` champs `--configuration-recorder` et.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> Groupe d'enregistrement et enregistreur de configuration
> Le champ `--recording-group` indique les types de ressources enregistrés.
> Le `--configuration-recorder` champ indique `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

1. Utilisez la commande `put-configuration-recorder` et spécifiez un ou plusieurs types de ressources dans le champ `resourceTypes` de `recordingGroup`, comme indiqué dans l'exemple suivant.
   i. Le fichier `recordingGroup.json` spécifie les types de ressources qui seront enregistrés par AWS Config .

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

> **Note**
>
> Champs obligatoires et facultatifs
>
> Avant de pouvoir spécifier les types de ressources à inclure dans l'enregistrement, vous devez définir les champs `allSupported` et `includeGlobalResourceTypes` sur `false` ou les omettre.
>
> Le champ `recordingStrategy` est facultatif lorsque vous répertoriez les types de ressources dans le champ `resourceTypes` de `--recording-group`.

> **Note**
>
> Disponibilité dans les Régions
>
> Avant de spécifier un type de ressource AWS Config à suivre, vérifiez la disponibilité des ressources par région pour voir si le type de ressource est pris en charge dans la AWS région où vous l'avez configuré AWS Config. Si un type de ressource est pris AWS Config en charge par au moins une région, vous pouvez activer l'enregistrement de ce type de ressource dans toutes les régions prises en charge AWS Config, même si le type de ressource spécifié n'est pas pris en charge dans la AWS région où vous l'avez configuré AWS Config.

ii. `put-configuration-recorder` utilise les champs suivants pour le paramètre `--configuration-recorder` :

- `name`— Nom de l'enregistreur de configuration. AWS Config attribue automatiquement le nom « par défaut » lors de la création de l'enregistreur de configuration.
- `roleARN`— Amazon Resource Name (ARN) du rôle IAM assumé AWS Config et utilisé par l'enregistreur de configuration.
- `recordingMode`— Spécifie la fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration. AWS Config prend en charge l'enregistrement continu et l'enregistrement quotidien. L'enregistrement en continu vous permet d'enregistrer les modifications de configuration en continu, chaque fois qu'un changement a lieu. L'enregistrement quotidien vous permet de recevoir un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il diffère de l'élément de configuration enregistré précédemment.

- `recordingFrequency`— Fréquence d'enregistrement par défaut AWS Config utilisée pour enregistrer les modifications de configuration.

  > **Note**
  >
  > AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d'enregistrement sur Continu.

- `recordingModeOverrides` : ce champ vous permet de définir vos exclusions pour le mode d'enregistrement. Il s'agit d'un tableau d'objets `recordingModeOverride`. Chaque objet `recordingModeOverride` du tableau `recordingModeOverrides` comprend trois champs :
  - `description` : description que vous fournissez pour l'exclusion.
  - `recordingFrequency` : fréquence d'enregistrement qui sera appliquée à tous les types de ressources spécifiés dans l'exclusion.
  - `resourceTypes`— Liste séparée par des virgules qui indique les types de ressources AWS Config inclus dans la dérogation.

> **Note**
>
> Champs obligatoires et facultatifs
> Le champ `recordingMode` pour `put-configuration-recorder` est facultatif. Par défaut, la fréquence d'enregistrement de l'enregistreur de configuration est définie sur Enregistrement en continu.

> **Note**
>
> Restrictions
> L'enregistrement quotidien ne prend pas en charge les types de ressources suivants :
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Pour la stratégie d'enregistrement Enregistrer tous les types de ressources actuels et futurs pris en charge (`ALL_SUPPORTED_RESOURCE_TYPES`), ces types de ressources seront définis sur Enregistrement en continu.

Le `configurationRecorder.json` fichier spécifie `name` et `roleArn` la fréquence d'enregistrement par défaut pour l'enregistreur de configuration (`recordingMode`). Vous pouvez également utiliser ce champ pour remplacer la fréquence d'enregistrement de types de ressources spécifiques.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Facultatif) Pour vérifier que votre enregistreur de configuration présente les paramètres souhaités, utilisez la commande `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

Voici un exemple de réponse.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
```

```
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Fréquence d’enregistrement

AWS Config prend en charge l'enregistrement continu et l'enregistrement quotidien. L’enregistrement en continu vous permet d’enregistrer les modifications de configuration en continu, chaque fois qu’un changement a lieu. L’enregistrement quotidien vous permet de recevoir un élément de configuration représentant l’état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s’il diffère de l’élément de configuration enregistré précédemment.

Enregistrement en continu

L’enregistrement en continu présente les avantages suivants :

- Surveillance en temps réel : l’enregistrement en continu permet de détecter immédiatement des changements non autorisés ou inattendus, ce qui peut renforcer vos efforts en matière de sécurité et de conformité.
- Analyse détaillée : l’enregistrement en continu vous permet d’analyser en profondeur les modifications apportées à la configuration de vos ressources au fur et à mesure qu’elles se produisent, ce qui peut vous permettre d’identifier les modèles et les tendances du moment.

Enregistrement quotidien

L’enregistrement quotidien présente les avantages suivants :

- Interruption minimale : l’enregistrement quotidien peut vous fournir un flux d’informations plus facile à gérer, et ainsi réduire la fréquence des notifications et la fatigue liée aux alertes.
- Rentabilité : l’enregistrement quotidien vous permet d’enregistrer les modifications apportées à vos ressources à une fréquence moindre, ce qui peut réduire les coûts liés au nombre de changements de configuration enregistrés.

> **Note**
>
> AWS Firewall Manager dépend de l'enregistrement continu pour surveiller vos ressources. Si vous utilisez Firewall Manager, il est recommandé de définir la fréquence d’enregistrement sur Continu.

Arrêt de l’enregistrement des ressources

Vous pouvez arrêter l'enregistrement AWS Config d'un type de ressource à tout moment. Après l' AWS Config arrêt de l'enregistrement d'une ressource, celle-ci conserve les informations de configuration précédemment capturées et vous pouvez continuer à accéder à ces informations.

Ressources non enregistrées

Si une ressource n'est pas enregistrée, AWS Config capture uniquement la création et la suppression de cette ressource, sans aucun autre détail, sans frais pour vous. Lorsqu'une ressource non enregistrée est créée ou supprimée, AWS Config envoie une notification et affiche l'événement sur

la page de détails de la ressource. La page des détails d'une ressource non enregistrée fournit des valeurs null pour la plupart des détails de configuration, et elle ne fournit pas d'informations sur les relations et les changements de configuration.

> **Note**
>
> Les types `AWS::IAM::User`, `AWS::IAM::Policy`, `AWS::IAM::Group` et `AWS::IAM::Role` captureront uniquement les états de création (`ResourceNotRecorded`) et de suppression (`ResourceDeletedNotRecorded`) si la ressource est, ou a déjà été, sélectionnée comme ressource à enregistrer dans l'enregistreur de configuration.

> **Note**
>
> Les éléments de configuration (CI) pour `ResourceNotRecorded` et `ResourceDeletedNotRecorded` ne suivent pas le temps d'enregistrement habituel pour les types de ressources. Ces types de ressources ne sont enregistrés que pendant le processus de référence périodique pour l'enregistreur de configuration, qui est moins fréquent que pour les autres types de ressources.

Les informations relationnelles qui AWS Config fournissent les ressources enregistrées ne sont pas limitées en raison des données manquantes pour les ressources non enregistrées. Si une ressource enregistrée est associée à une ressource non enregistrée, cette relation est mentionnée dans la page des caractéristiques de la ressource enregistrée.

AWS Config Règles et types de ressources globaux

Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources IAM globaux ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations

dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Meilleures pratiques pour rendre compte de la conformité des ressources mondiales intégrées avant février 2022

Pour éviter des évaluations inutiles, vous devez uniquement déployer AWS Config les règles et les packs de conformité qui incluent ces ressources globales dans l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions. Cela s'applique aux AWS Config règles, aux AWS Config règles organisationnelles, ainsi qu'aux règles créées par d'autres AWS services, tels que AWS Security Hub et AWS Control Tower.

Si vous n’enregistrez pas les types de ressources mondiales intégrés avant février 2022, nous vous recommandons de ne pas activer les règles périodiques suivantes afin d’éviter des évaluations inutiles :

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

Meilleures pratiques pour rendre compte de la conformité des ressources mondiales intégrées après février 2022

Les types de ressources globales intégrés à AWS Config l'enregistrement après février 2022 seront enregistrés uniquement dans la région d'origine du service pour la partition commerciale et AWS GovCloud (ouest des États-Unis) pour la partition. AWS GovCloud (US) Vous devez déployer AWS Config des règles et des packs de conformité qui concernent ces ressources globales uniquement

dans la région d'origine du type de ressource. Pour plus d'informations, voir Régions d'origine pour les types de ressources globaux.

Enregistrement de configurations pour les ressources tierces

Enregistrez les configurations pour les ressources tierces ou les types de ressources personnalisés tels que les serveurs sur site, les outils de surveillance SAAS et les systèmes de contrôle de version (similaires GitHub). Vous pouvez publier les données de configuration de ressources tierces, consulter AWS Config et surveiller l'inventaire des ressources et l'historique de configuration à l'aide de AWS Config la console et des API. Vous pouvez désormais les utiliser AWS Config pour gérer toutes vos ressources et évaluer la configuration des ressources pour en vérifier la conformité par rapport aux meilleures pratiques en utilisant des AWS Config règles. Vous pouvez également créer des AWS Config règles ou des packs de conformité pour évaluer ces ressources tierces par rapport aux meilleures pratiques, aux politiques internes et aux politiques réglementaires.

> **Note**
>
> Si vous avez configuré AWS Config pour enregistrer tous les types de ressources, les ressources tierces qui sont gérées (créées, mises à jour ou supprimées) AWS CloudFormation sont automatiquement suivies en AWS Config tant qu'éléments de configuration.

Prérequis : les ressources tierces ou le type de ressource personnalisé doivent être enregistrés à l'aide de AWS CloudFormation.

Rubriques

- Étape 1 : Configurer votre environnement de développement
- Étape 2 : Modéliser votre ressource
- Étape 3 : Générer des artefacts
- Étape 4 : Enregistrer la ressource
- Étape 5 : Publier la configuration des ressources
- Enregistrer et supprimer un état de configuration pour des ressources tierces à l'aide de AWS CLI
- Gestion d'un état de configuration pour le type de ressources tierces à l'aide d'API

Étape 1 : Configurer votre environnement de développement

Installez et configurez AWS CloudFormation AWS CLI. Vous AWS CLI permet de modéliser et d'enregistrer vos ressources personnalisées. Pour plus d'informations, voir Ressources personnalisées et Qu'est-ce que l'interface de ligne de CloudFormation commande ? .

Étape 2 : Modéliser votre ressource

Créez un schéma de fournisseur de ressources conforme à la configuration du type de ressource et valide.

1. Utilisez la commande `init` pour créer votre projet de fournisseur de ressources et générer les fichiers nécessaires.

```
$ cfn init
Initializing new project
```

2. La commande `init` lance un assistant qui vous guide tout au long de la configuration du projet, y compris lors de la spécification du nom de la ressource. Pour cette procédure pas à pas, spécifiez `MyCustomNamespace::Testing::WordPress`.

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. Entrez un nom de package pour votre ressource.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> Afin de garantir la résolution appropriée de toutes les dépendances du projet, vous pouvez importer le projet généré dans votre IDE avec la prise en charge de Maven. Par exemple, si vous utilisez IntelliJ IDEA, il se peut que vous deviez suivre la procédure suivante :
>
> - Dans le menu Fichier, choisissez Nouveau, puis Projet provenant de sources existantes.

- Accédez au répertoire du projet
- Dans la boîte de dialogue Importer un projet, choisissez Importer un projet depuis un modèle externe, puis sélectionnez Maven.
- Choisissez Suivant et acceptez toutes les valeurs par défaut pour terminer l'importation du projet.

4. Ouvrez le fichier `mycustomnamespace-testing-wordpress.json` qui contient le schéma de votre ressource. Copiez et collez le schéma suivant dans `mycustomnamespace-testing-wordpress.json`.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Validez le schéma.

```
$ cfn validate
```

6. Mettez à jour les fichiers générés automatiquement dans le package du fournisseur de ressources pour afficher les mises à jour du schéma du fournisseur de ressources. Lors du lancement du projet de fournisseur de ressources, il AWS CLI génère des fichiers de support et du code pour le fournisseur de ressources. Régénérez le code pour voir le schéma mis à jour.

```
$ cfn generate
```

> **Note**
>
> Lorsque vous utilisez Maven, dans le cadre du processus de création, la commande `generate` est automatiquement exécutée avant que le code ne soit compilé. Ainsi, vos modifications ne seront jamais désynchronisées avec le code généré.
> Sachez que la CloudFormation CLI doit se trouver dans un emplacement que Maven/le système peut trouver. Pour plus d'informations, consultez Configuration de votre environnement pour les extensions de développement.

Pour plus d'informations sur l'ensemble du processus, consultez Modélisation des fournisseurs de ressources à utiliser dans AWS CloudFormation.

Étape 3 : Générer des artefacts

Exécutez la commande suivante pour générer des artefacts pour `cfn submit`.

```
$ mvn package
```

Étape 4 : Enregistrer la ressource

AWS Config ne nécessite pas que les gestionnaires de fournisseurs de ressources effectuent le suivi de la configuration de votre ressource. Exécutez la commande suivante pour enregistrer votre ressource.

```
$ cfn submit
```

Pour plus d'informations, consultez la section Enregistrement des fournisseurs de ressources à utiliser dans les AWS CloudFormation modèles.

Étape 5 : Publier la configuration des ressources

Déterminez la configuration pour MyCustomNamespace ::Testing : :WordPress.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Déterminez l'identifiant de version du schéma à partir de AWS CloudFormation `DescribeType`.

AWS Config Pour voir si cette configuration de ressource est acceptée. Pour évaluer la conformité, vous pouvez rédiger AWS Config des règles à l'aide de cette ressource. Pour plus d'informations, voir Enregistrer et supprimer un état de configuration pour des ressources tierces à l'aide de la AWS CLI.

Facultatif : pour automatiser l'enregistrement de la configuration, implémentez des collecteurs de configuration périodique ou basés sur les modifications.

Enregistrer et supprimer un état de configuration pour des ressources tierces à l'aide de AWS CLI

AWS CLI Il s'agit d'un outil unifié pour gérer vos AWS services. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs AWS services depuis la ligne de commande et utiliser des scripts pour les automatiser. Pour plus d'informations sur les AWS CLI outils AWS CLI et pour obtenir des instructions sur leur installation, reportez-vous à ce qui suit dans le guide de AWS Command Line Interface l'utilisateur.

- AWS Command Line Interface Guide de l'utilisateur
- Préparation de l’installation de l’ AWS Command Line Interface

Si nécessaire, entrez `aws configure` pour configurer le AWS CLI afin d'utiliser une AWS région dans laquelle AWS Config des agrégateurs sont disponibles.

Rubriques

- Enregistrement d'un élément de configuration
- Lecture de l'élément de configuration à l'aide des API AWS Config
- Suppression de la ressource tierce

Enregistrement d'un élément de configuration

Enregistrez un élément de configuration pour une ressource tierce ou un type de ressource personnalisé à l'aide de la procédure suivante :

Assurez-vous d'enregistrer le type de ressource `MyCustomNamespace::Testing::WordPress` avec le schéma qui lui correspond.

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez la commande suivante :

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> Tel que défini dans le schéma de type, `writeOnlyProperties` sera supprimé de la configuration avant d'être enregistré par AWS Config. Par conséquent, ces valeurs ne seront pas présentes lorsque la configuration sera obtenue via des API de lecture. Pour plus d'informations sur `writeOnlyProperties`, consultez Schéma du type de ressource.

Lecture de l'élément de configuration à l'aide des API AWS Config

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez la commande suivante :

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Appuyez sur Entrée.

   Vous devez voir des résultats similaires à ce qui suit :

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. Entrez la commande suivante :

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Appuyez sur Entrée.

   Vous devez voir des résultats similaires à ce qui suit :

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
```

```
    ]
}
```

Suppression de la ressource tierce

Vous pouvez enregistrer l'état de configuration d'un type de ressource tiers ou personnalisé que vous souhaitez supprimer.

- Entrez la commande suivante :

  ```
  aws configservice delete-resource-config --resource-type
   MyCustomNamespace::Testing::WordPress --resource-id resource-002
  ```

  En cas de réussite, la commande s'exécute sans sortie supplémentaire.

Gestion d'un état de configuration pour le type de ressources tierces à l'aide d'API

Vous pouvez gérer un état de configuration pour des ressources tierces ou un type de ressource personnalisé à l'aide des API PutResourceDeleteResourceConfig et Config. Pour plus d’informations, consultez la page Référence de l’API .

- PutResourceConfig
- DeleteResourceConfig

Enregistrement de la configuration logicielle pour des instances gérées

Vous pouvez l'utiliser AWS Config pour enregistrer les modifications de l'inventaire des logiciels sur les instances Amazon EC2 et les serveurs sur site. Cela vous permet de voir les modifications qui ont été apportées à la configuration logicielle. Par exemple, lorsqu'une nouvelle mise à jour Windows est installée sur une instance Windows gérée, AWS Config enregistre les modifications, puis les envoie à votre canal de diffusion, afin que vous soyez informé de la modification. Avec AWS Config, vous pouvez consulter l'historique des mises à jour Windows installées pour l'instance gérée et leur évolution au fil du temps.

Vous devez effectuer les étapes suivantes pour enregistrer les modifications apportées à la configuration logicielle :

- Activez l'enregistrement pour le type de ressource Inventaire des instances gérées dans AWS Config.
- Configurez les instances EC2 et les serveurs sur site comme instances gérées dans AWS Systems Manager. Une instance gérée est une machine qui a été configurée pour une utilisation avec Systems Manager.
- Lancez l'extraction des inventaires logiciels sur vos instances gérées à l'aide de la fonctionnalité Systems Manager Inventory.

> **Note**
>
> Systems Manager prend désormais en charge la création d'éléments de configuration pour les instances non gérées
> L'élément de configuration pour les instances non gérées aura une configuration supplémentaire avec `Key: “InstanceStatus”` et `Value: “Unmanaged”`.
> Les éléments de configuration pour les instances non gérées ne recevront pas de mises à jour supplémentaires
> Pour recevoir des mises à jour supplémentaires, l'élément de configuration doit être une instance gérée.

Vous pouvez également utiliser AWS Config des règles pour surveiller les modifications de configuration logicielle et être averti si les modifications sont conformes ou non à vos règles. Par exemple, si vous créez une règle qui vérifie si une application spécifique est installée sur vos instances gérées, cette application n'est pas installée sur une instance, AWS Config signale cette instance comme non conforme à votre règle. Pour obtenir la liste des règles AWS Config gérées, consultezListe des règles AWS Config gérées.

Pour activer l'enregistrement des modifications de configuration des logiciels dans AWS Config :

1. Activez l'enregistrement pour tous les types de ressource pris en charge ou sélectionnez précisément le type de ressource Inventaire des instances gérées dans AWS Config. Pour plus d’informations, consultez AWS Ressources d'enregistrement.

2. Lancez une instance Amazon EC2 avec un profil d'instance pour Systems Manager qui inclut la politique gérée par AmazonSSM ManagedInstanceCore. Cette politique gérée AWS permet à une instance d'utiliser les fonctions de base du service Systems Manager.

   Pour plus d'informations sur les autres politiques que vous pouvez ajouter au profil d'instance pour Systems Manager, consultez Création d'un profil d'instance IAM pour Systems Manager dans le Guide de l'utilisateur AWS Systems Manager .

   > **Important**
   >
   > L'agent SSM est un logiciel Amazon qui doit être installé sur une instance gérée afin de communiquer avec Systems Manager dans le cloud. Si votre instance EC2 a été créée à partir d'une AMI pour l'un des systèmes d'exploitation suivants, l'agent est préinstallé :
   >
   > - AMI Windows Server 2003-2012 R2 publiées en novembre 2016 ou ultérieurement
   > - Windows Server 2016 et 2019
   > - Amazon Linux
   > - Amazon Linux 2
   > - Ubuntu Server 16.04
   > - Ubuntu Server 18.04
   >
   > Sur les instances EC2 qui n'ont pas été créées à partir d'une AMI avec l'agent préinstallé, vous devez installer l'agent manuellement. Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur AWS Systems Manager :
   >
   > - Installation et configuration de SSM Agent sur des instances EC2 pour Windows Server
   > - Installation et configuration de SSM Agent sur des instances EC2 pour Linux

3. Lancez la collecte d'inventaire comme décrit dans Configuration de la collecte d'inventaire dans le Guide de l'utilisateur AWS Systems Manager . Les procédures sont les mêmes pour les instances Linux et Windows.

   AWS Config peut enregistrer les modifications de configuration pour les types d'inventaire suivants :

   - Applications – Liste d'applications pour les instances gérées, par exemple, un logiciel antivirus.

- AWS composants : liste de AWS composants pour les instances gérées, tels que les SDK AWS CLI et.
- Informations sur l'instance – Informations sur l'instance, par exemple, nom et version du système d'exploitation, domaine et état du pare-feu.
- Configuration du réseau – Informations de configuration telles que l'adresse IP, la passerelle et le masque de sous-réseau.
- Mises à jour Windows – Liste des mises à jour Windows pour les instances gérées (instances Windows uniquement).

> **Note**
>
> AWS Config ne prend pas en charge l'enregistrement du type d'inventaire personnalisé pour le moment.

L'extraction des inventaires est l'une des nombreuses fonctionnalités Systems Manager, qui sont regroupées dans les catégories Gestion des opérations, Actions et modification, Instances et nœuds et Ressources partagées. Pour plus d'informations, consultez Qu'est-ce que Systems Manager ? et Fonctionnalités de Systems Manager dans le Guide de l'utilisateur AWS Systems Manager .

Affichage des configurations de ressource et de l'historique

Vous pouvez consulter toutes les ressources enregistrées AWS Config dans votre compte, les modifications de configuration apportées à une ressource sur une période donnée, ainsi que les relations entre la ressource sélectionnée et toutes les ressources associées. Vous pouvez également consulter les modifications de l'état de conformité des ressources telles qu'elles ont été évaluées en les AWS Config Rules affichant dans une chronologie.

Rubriques

- Recherche de ressources découvertes par AWS Config
- Affichage des informations de conformité et des résultats d'évaluation
- Affichage de l'historique de configuration et de conformité

Recherche de ressources découvertes par AWS Config

Vous pouvez utiliser la AWS Config console et l' AWS Config API pour rechercher les ressources qui ont AWS Config été inventoriées ou découvertes, y compris les ressources supprimées et les ressources qui ne AWS Config sont pas en cours d'enregistrement. AWS CLI AWS Config découvre uniquement les types de ressources pris en charge. Pour plus d'informations, consultez Types de ressource pris en charge.

Recherche de ressources (Console)

Vous pouvez utiliser les types de ressource ou les informations de balises pour rechercher des ressources dans la console AWS Config .

Pour rechercher des ressources (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Sur la page Inventaire des ressources, spécifiez les options de recherche pour les ressources que vous souhaitez rechercher :
   - Catégorie de ressources : choisissez toutes les catégories de ressources ou limitez les résultats aux seules AWS ressources.
   - Type de ressource : choisissez tous les types de ressources ou sélectionnez la ou les ressource(s) à filtrer.
   - Conformité : choisissez de filtrer selon l'état de conformité, conforme ou non conforme.
3. AWS Config répertorie les ressources correspondant à vos options de recherche. Vous pouvez voir les informations suivantes sur les ressources :
   - Identifiant de ressource : l'identifiant de ressource peut être un ID de ressource ou un nom de ressource, le cas échéant. Choisissez le lien de l'identifiant d'une ressource pour afficher la page de détails de cette ressource.
   - Type de ressource : le type de la ressource est répertorié.
   - Conformité : statut de la ressource AWS Config évaluée par rapport à votre règle.

     Pour plus d'informations, consultez Affichage de l'historique de configuration et de conformité.

Recherche de ressources (AWS CLI)

Vous pouvez utiliser le AWS CLI pour répertorier les AWS Config ressources découvertes.

Pour rechercher des ressources (AWS CLI)

Utilisez la commande AWS Config service **`list-discovered-resources`** :

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

Pour afficher les détails de configuration d'une ressource répertoriée dans la réponse, utilisez la commande `get-resource-config-history` et spécifiez le type de ressource et l'ID de ressource. Pour un exemple de cette commande et de la réponse de AWS Config, consultezAffichage de l'historique de configuration.

Recherche de ressources (API)

Vous spécifiez un type de ressource et vous AWS Config renvoyez une liste d'identificateurs de ressources pour les ressources de ce type. Pour plus d'informations, consultez ResourceIdentifierla référence de AWS Config l'API.

Pour rechercher des ressources (API)

Utilisez l'action ListDiscoveredResources.

Pour obtenir les détails de configuration d'une ressource répertoriée dans la réponse, utilisez l'GetResourceConfigHistoryaction et spécifiez le type et l'ID de la ressource.

Affichage des informations de conformité et des résultats d'évaluation

> **Important**
>
> Pour obtenir des rapports précis sur l'état de conformité, vous devez enregistrer le type de ressource `AWS::Config::ResourceCompliance`. Pour plus d'informations, consultez la section AWS Ressources de recodage.

Vous pouvez utiliser la AWS Config console ou AWS les SDK pour consulter les informations de conformité et les résultats de l'évaluation de vos règles et ressources.

Table des matières

- Affichage de la conformité (console)
- Visualisation de la conformité (AWS SDK)

Affichage de la conformité (console)

Pour vérifier la conformité (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région qui prend en charge les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le panneau de navigation, choisissez Resources (Ressources). Sur la page Inventaire des ressources, vous pouvez filtrer par catégorie de ressource, type de ressource et état de conformité. Choisissez Inclure les ressources supprimées, le cas échéant. La tableau affiche l'identifiant de ressource correspondant au type de ressource ainsi que l'état de conformité de cette ressource. L'identifiant de ressource peut être un ID de ressource ou un nom de ressource.
4. Choisissez une ressource dans la colonne des identifiants de ressource.
5. Cliquez sur le bouton Chronologie des ressources. Vous pouvez filtrer par événements de configuration, événements de conformité ou CloudTrail événements.

> **Note**
>
> Sinon, sur la page Inventaire des ressources, vous pouvez directement choisir le nom de la ressource. Pour accéder à la chronologie des ressources depuis la page des détails des ressources, cliquez sur le bouton Chronologie des ressources.

Vous pouvez aussi afficher la conformité de vos ressources en les examinant dans la page Resource inventory (Inventaire des ressources). Pour plus d'informations, consultez Recherche de ressources découvertes par AWS Config.

Visualisation de la conformité (AWS SDK)

Pour obtenir des informations sur la conformité de vos AWS Config règles

Les exemples de code suivants montrent comment utiliser`DescribeComplianceByConfigRule`.

CLI

AWS CLI

Pour obtenir des informations de conformité pour vos règles de AWS Config

La commande suivante renvoie des informations de conformité pour chaque règle de AWS Config violée par une ou plusieurs AWS ressources :

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de ressources qui ne sont pas conformes à la règle correspondante. Par exemple, le résultat suivant indique que 3 ressources ne sont pas conformes à la règle nommée`InstanceTypesAreT2micro`.

Sortie :

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
```

```
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByConfigRuleà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple récupère les détails de conformité de la règle ebs-optimized-instance, pour laquelle il n'existe aucun résultat d'évaluation actuel pour la règle, il renvoie donc INSUSUFFISENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Sortie :

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Exemple 2 : Cet exemple renvoie le nombre de ressources non conformes pour la règle ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Sortie :

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByConfigRuleà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir des informations de conformité pour vos AWS ressources

Les exemples de code suivants montrent comment utiliser`DescribeComplianceByResource`.

CLI

AWS CLI

Pour obtenir des informations de conformité pour vos AWS ressources

La commande suivante renvoie des informations de conformité pour chaque instance EC2 enregistrée par AWS Config et qui enfreint une ou plusieurs règles :

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Dans le résultat, la valeur de chaque `CappedCount` attribut indique le nombre de règles violées par la ressource. Par exemple, le résultat suivant indique que l'instance `i-1a2b3c4d` enfreint 2 règles.

Sortie :

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
```

```
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByResourceà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple vérifie le type de **`AWS::SSM::ManagedInstanceInventory`** ressource pour le type de conformité « COMPLIANT ».

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Sortie :

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
```

```
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByResourceà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir le résumé de conformité de vos AWS Config règles

Les exemples de code suivants montrent comment utiliser`GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Pour obtenir le résumé de conformité de vos règles de AWS Config

La commande suivante renvoie le nombre de règles conformes et le nombre de règles non conformes :

```
aws configservice get-compliance-summary-by-config-rule
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de règles conformes ou non conformes.

Sortie :

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByConfigRuleà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie le nombre de règles Config non conformes.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Sortie :

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByConfigRuleà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir le résumé de conformité de vos AWS ressources

Les exemples de code suivants montrent comment utiliser`GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Pour obtenir le résumé de conformité pour tous les types de ressources

La commande suivante renvoie le nombre de AWS ressources non conformes et le nombre de ressources conformes :

```
aws configservice get-compliance-summary-by-resource-type
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de ressources conformes ou non conformes.

Sortie :

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Pour obtenir le résumé de conformité pour un type de ressource spécifique

La commande suivante renvoie le nombre d'instances EC2 non conformes et le nombre d'instances conformes :

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de ressources conformes ou non conformes.

Sortie :

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
```

```
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByResourceTypeà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie le nombre de ressources conformes ou non conformes et convertit la sortie en json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByResourceTypeà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir les résultats de l'évaluation d'une AWS Config règle

Les exemples de code suivants montrent comment utiliser`GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Pour obtenir les résultats de l'évaluation d'une règle AWS Config

La commande suivante renvoie les résultats de l'évaluation pour toutes les ressources qui ne sont pas conformes à une règle de AWS configuration nommée `InstanceTypesAreT2micro` :

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Sortie :

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
```

```
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByConfigRuleà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple obtient les résultats de l'évaluation de la règle access-keys-rotated et renvoie la sortie groupée par type de conformité

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Sortie :

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Exemple 2 : Cet exemple interroge les détails de conformité de la règle relative access-keys-rotated aux ressources COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Sortie :

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByConfigRuleà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir les résultats de l'évaluation d'une AWS ressource

Les exemples de code suivants montrent comment utiliser`GetComplianceDetailsByResource`.

CLI

AWS CLI

Pour obtenir les résultats de l'évaluation d'une AWS ressource

La commande suivante renvoie les résultats de l'évaluation pour chaque règle à laquelle l'instance EC2 n'est `i-1a2b3c4d` pas conforme :

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Sortie :

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
```

```
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByResourceà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple d'évaluation donne des résultats pour la ressource donnée.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Sortie :

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
```

```
ResultToken                :
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByResourceà la section Référence des AWS Tools for PowerShell applets de commande.

Affichage de l'historique de configuration et de conformité

> **Important**
>
> Pour obtenir des rapports précis sur l'état de conformité, vous devez enregistrer le type de ressource `AWS::Config::ResourceCompliance`. Pour plus d'informations, consultez la section AWS Ressources de recodage.

Vous pouvez consulter la configuration, les relations et le nombre de modifications apportées à une ressource dans la AWS Config console. Vous pouvez consulter l'historique de configuration d'une ressource à l'aide de AWS CLI.

Affichage des détails de configuration (console)

Affichage des détails de configuration à l'aide de la console

Lorsque vous recherchez des ressources sur la page Inventaire des ressources, choisissez le nom ou l'ID de la ressource dans la colonne des identifiants de ressource pour afficher la page de détails de la ressource. La page des détails fournit des informations sur la configuration, les relations et le nombre de modifications apportées à cette ressource.

Pour accéder à la chronologie des ressources depuis la page des détails des ressources, cliquez sur le bouton Chronologie des ressources. Cette chronologie des ressources capture les modifications sous forme d'éléments `ConfigurationItems` sur une période de temps pour une ressource spécifique. Vous pouvez filtrer par événements de configuration, événements de conformité ou CloudTrail événements.

Affichage des détails de configuration (AWS CLI)

Affichage des détails de configuration à l'aide du AWS CLI

Les éléments de configuration enregistrés AWS Config sont fournis au canal de distribution spécifié à la demande sous forme d'instantané de configuration et de flux de configuration. Vous pouvez utiliser le AWS CLI pour afficher l'historique des éléments de configuration pour chaque ressource.

Affichage de l'historique de configuration

Entrez la commande `get-resource-config-history` et spécifiez le type de ressource et l'ID de ressource, par exemple :

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
```

```
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

Pour une explication détaillée des champs réponse, consultez Components of a Configuration Item et Types de ressource pris en charge.

Exemple d'historique de configuration Amazon EBS; issu de AWS Config

AWS Config génère un ensemble de fichiers représentant chacun un type de ressource et répertorie toutes les modifications de configuration pour les ressources de ce type en cours AWS Config d'enregistrement. AWS Config exporte cet historique de configuration centré sur les ressources sous forme d'objet dans le compartiment Amazon S3 que vous avez spécifié lors de l'activation. AWS Config Le fichier d'historique de configuration pour chaque type de ressource contient les modifications qui ont été détectées pour les ressources de ce type depuis l'obtention du dernier fichier d'historique. En général, les fichiers d'historique sont fournis toutes les six heures.

Voici un exemple du contenu de l'objet Amazon S3 qui décrit l'historique de configuration de tous les volumes Amazon Elastic Block Store de la région actuelle pour votre Compte AWS. Ce compte comportent les volumes `vol-ce676ccc` et `vol-cia007c`. Le volume `vol-ce676ccc` a connu deux modifications de configuration depuis l'obtention du fichier d'historique alors que le volume `vol-cia007c` n'en a connu qu'une.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
```

```
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
```

```
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-ad229edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
```

```
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "vol-cia007c",
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
        "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a67u292281"
        ],
        "availibilityZone": "us-west-2b",
        "resourceType": "AWS::EC2::Volume",
        "resourceCreationTime": "2014-02-27T20:43:53.885Z",
        "tags": {},
        "relationships": [
            {
                "resourceId": "i-344e563d",
                "resourceType": "AWS::EC2::Instance",
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-cia007c",
```

```
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

Affichage de la chronologie de l'historique de conformité pour les ressources

AWS Config prend en charge le stockage des modifications de l'état de conformité des ressources telles qu'évaluées par AWS Config Rules. L'historique de conformité de ressource se présente sous la forme d'une chronologie. Cette chronologie capture les modifications sous forme d'éléments `ConfigurationItems` sur une période de temps pour une ressource spécifique. Pour plus d'informations sur le contenu de`ConfigurationItem`, consultez ConfigurationItemla référence de l' AWS Config API.

Vous pouvez accepter ou refuser l'enregistrement de tous les types de ressources dans AWS Config. Si vous avez choisi d'enregistrer tous les types de ressources, commence AWS Config

automatiquement à enregistrer l'historique de conformité des ressources tel qu'évalué par AWS Config Rules. Par défaut, AWS Config enregistre les modifications de configuration pour toutes les ressources prises en charge. Vous pouvez également sélectionner uniquement le type de ressource spécifique de l'historique de conformité des ressources : `AWS::Config::ResourceCompliance`. Pour plus d'informations, voir Sélection des AWS Config enregistrements de ressources.

Affichage de la chronologie des ressources à l'aide des ressources

Accédez à la chronologie des ressources en sélectionnant une ressource spécifique à partir de la page d'inventaire des ressources.

1. Sélectionnez les ressources dans le volet de navigation de gauche.
2. Sur la page Inventaire des ressources, vous pouvez filtrer par catégorie de ressource, type de ressource et état de conformité. Choisissez Inclure les ressources supprimées, le cas échéant.

   La tableau affiche l'identifiant de ressource correspondant au type de ressource ainsi que l'état de conformité de cette ressource. L'identifiant de ressource peut être un ID de ressource ou un nom de ressource.
3. Choisissez une ressource dans la colonne des identifiants de ressource.
4. Cliquez sur le bouton Chronologie des ressources. Vous pouvez filtrer par événements de configuration, événements de conformité ou CloudTrail événements.

   > **Note**
   >
   > Sinon, sur la page Inventaire des ressources, vous pouvez directement choisir le nom de la ressource. Pour accéder à la chronologie des ressources depuis la page des détails des ressources, cliquez sur le bouton Chronologie des ressources.

Affichage de la chronologie des ressources à l'aide des règles

Accédez à la chronologie de conformité en sélectionnant une règle spécifique dans la page Règle.

1. Sélectionnez les règles dans le volet de navigation de gauche.
2. Sur la page Règle, choisissez une règle qui évalue les ressources qui vous intéressent. Si aucune règle ne s'affiche à l'écran, ajoutez-en à l'aide du bouton Ajouter une règle.
3. Sur la page de détails de la règle, sélectionnez les ressources dans le tableau des ressources évaluées.

4. Cliquez sur le bouton Chronologie des ressources. La chronologie des ressources s'affiche.

Interrogation de l'historique de conformité

Interrogez l'historique de conformité des ressources à get-resource-config-history l'aide du type de ressource`AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

Vous devez voir des résultats similaires à ce qui suit :

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
    }
   ]
   "tags": {},
   "resourceType": "AWS::Config::ResourceCompliance",
   "resourceId": "AWS::S3::Bucket/configrules-bucket",
   "ConfigurationStateId": "1539799966921",
   "relatedEvents": [];
   "awsRegion": "us-west-2",
   "version": "1.3",
   "configurationItemMD5Hash": "",
   "supplementaryConfiguration": {},
   "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

   "configurationItemStatus": "ResourceDiscovered",
   "accountId": "AccountID"
  }
 ]
```

```
}
```

Balisage de vos ressources AWS Config

Une balise est une étiquette que vous affectez à une ressource AWS. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez. Les balises facilitent la gestion, la recherche et le filtrage des ressources.

Les étiquettes vous permettent de classer vos ressources AWS de différentes manières, par exemple, par objectif, par propriétaire ou par environnement. Cela s'avère utile quand il existe un grand nombre de ressources du même type : vous pouvez identifier rapidement une ressource spécifique en fonction des balises que vous lui avez attribuées. Vous pouvez attribuer une ou plusieurs balises à vosAWS ressources. Chaque balise possède une valeur associée.

Nous vous recommandons de concevoir un ensemble de clés d'étiquette répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de vos ressources. Gestion de vosAWS ressources. Vous pouvez rechercher et filtrer les ressources en fonction des étiquettes que vous ajoutez.

Les balises sont interprétées strictement en tant que chaîne de caractères et ne sont pas automatiquement affectées à vos ressources. Vous pouvez modifier les clés et valeurs d'identification, et vous pouvez retirer des identifications d'une ressource à tout moment. Vous pouvez définir la valeur d'une balise sur une chaîne vide, mais vous ne pouvez pas définir la valeur d'une balise sur null. Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur. Si vous supprimez une ressource, les balises associées à celle-ci seront également supprimées.

Vous pouvez gérer les balises à l'aide de l'AWS Command Line Interface (AWS CLI) et de la référence d'API AWS Config.

Restrictions liées au balisage

Les restrictions de base suivantes s'appliquent aux balises.

Restriction	Description
Nombre maximal de balises par ressource	50

Restriction	Description
Longueur maximale de clé	128 caractères Unicode en UTF-8
Longueur maximale de valeur	256 caractères Unicode en UTF-8
Restriction de préfixe	N'utilisez pas le préfixe `aws:` dans les noms ou valeurs des balises, car celui-ci est réservé pour être utilisé par AWS. Vous ne pouvez pas modifier ou supprimer des noms ou valeurs de balise ayant ce préfixe. Les balises avec ce préfixe ne sont pas comptabilisées comme vos balises pour la limite de ressources.
Restrictions de caractères	Les balises doivent contenir uniquement des lettres Unicode, des chiffres, des espaces ou les symboles : `_ . : / = + - @`

Gestion des balises à l'aide des actions d'API AWS Config

Des contrôles d'accès basés sur les balises sont disponibles pour les trois ressources `ConfigurationAggregator`, `AggregationAuthorization` et `ConfigRule`. Utilisez les commandes suivantes pour ajouter, mettre à jour, répertorier et supprimer les étiquettes pour vos ressources.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResourceetUntagResource` nécessitent certaines autorisationsAWS Identity and Access Management (IAM) pour contrôler l'accès. Pour de plus amples informations, veuillez consulter Contrôle de l'accès à l'aide des balises du Guide de l'utilisateur IAM.

Évaluation des ressources à l'aide de AWS Config règles

AWS Config À utiliser pour évaluer les paramètres de configuration de vos AWS ressources. Pour ce faire, vous devez créer AWS Config des règles qui représentent vos paramètres de configuration idéaux. AWS Config fournit des règles prédéfinies personnalisables appelées règles gérées pour vous aider à démarrer.

Comment fonctionnent AWS Config les règles

Pendant qu' AWS Config surveille en permanence les changements de configuration de vos ressources, il vérifie si ces changements vont à l'encontre de l'une des conditions de vos règles. Si une ressource n'est pas conforme à la règle, AWS Config marque la ressource et la règle comme non conformes. Les résultats d'évaluation possibles pour une AWS Config règle sont les suivants :

- `COMPLIANT` - la règle satisfait aux conditions du contrôle de conformité.
- `NON_COMPLIANT` - la règle ne satisfait pas aux conditions du contrôle de conformité.
- `ERROR` - l'un des paramètres obligatoires/facultatifs n'est pas valide, n'est pas du bon type ou est mal formaté.
- `NOT_APPLICABLE` - utilisé pour filtrer les ressources auxquelles la logique de la règle ne peut s'appliquer. Par exemple, la règle alb-desync-mode-check ne vérifie que les Application Load Balancers et ignore les Network Load Balancers et les équilibreurs de charge de passerelle.

Par exemple, lorsqu'un volume EC2 est créé, AWS Config vous pouvez évaluer le volume par rapport à une règle qui exige que les volumes soient chiffrés. Si le volume n'est pas chiffré, AWS Config marque le volume et la règle comme non conformes. AWS Config peut également vérifier toutes vos ressources pour vérifier les exigences applicables à l'ensemble du compte. Par exemple, AWS Config vous pouvez vérifier si le nombre de volumes EC2 d'un compte reste dans les limites du total souhaité ou si un compte les utilise à des AWS CloudTrail fins de journalisation.

Règles liées aux services

Les règles liées aux services constituent un type unique de règle gérée qui permet à d'autres AWS services de créer des AWS Config règles dans votre compte. Ces règles sont prédéfinies pour inclure toutes les autorisations requises pour appeler d'autres AWS services en votre nom. Ces règles sont similaires aux normes qu'un AWS service vous recommande Compte AWS pour la vérification de conformité. Pour plus d’informations, consultez Règles liées aux services AWS Config.

Règles personnalisées

Vous pouvez également créer des règles personnalisées pour évaluer les ressources supplémentaires qui AWS Config ne sont pas encore enregistrées. Pour plus d'informations, consultez AWS Config Règles personnalisées et Évaluation des types de ressources supplémentaires.

Affichage de la conformité

La AWS Config console indique l'état de conformité de vos règles et de vos ressources. Vous pouvez voir dans quelle mesure vos AWS ressources sont globalement conformes aux configurations souhaitées et savoir quelles ressources spécifiques ne sont pas conformes. Vous pouvez également utiliser la AWS CLI, l' AWS Config API et AWS les SDK pour demander au AWS Config service des informations de conformité.

En utilisant AWS Config pour évaluer vos configurations de ressources, vous pouvez évaluer dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.

Limites

Pour connaître le nombre maximum de AWS Config règles par région pour chaque compte et les autres limites de service, consultez la section Limites AWS Config de service.

Considérations de coût

Pour plus de détails sur les coûts associés à l'enregistrement des ressources, consultez la section AWS Config tarification.

Recommandation : arrêtez d'enregistrer la conformité des ressources avant de supprimer les règles

Il est vivement recommandé d'arrêter l'enregistrement pour le type de `AWS::Config::ResourceCompliance` ressource avant de supprimer les règles de votre compte. La suppression de règles crée des éléments de configuration (CI) pour votre enregistreur de configuration `AWS::Config::ResourceCompliance` et peut avoir une incidence sur les coûts AWS Config de votre enregistreur de configuration. Si vous supprimez des règles qui évaluent un grand nombre de types de ressources, cela peut entraîner une augmentation du nombre de CI enregistrés.

Bonnes pratiques :

1. Arrêter l'enregistrement `AWS::Config::ResourceCompliance`

2. Supprimer une ou plusieurs règles
3. Activez l'enregistrement pour `AWS::Config::ResourceCompliance`

Recommandation : ajouter une logique pour gérer l'évaluation des ressources supprimées pour les règles Lambda personnalisées

Lorsque vous créez AWS Config des règles lambda personnalisées, il est vivement recommandé d'ajouter une logique pour gérer l'évaluation des ressources supprimées.

Lorsque les résultats de l'évaluation sont marqués comme `NOT_APPLICABLE`, ils seront marqués pour suppression et nettoyés. S'ils ne sont PAS marqués comme tels`NOT_APPLICABLE`, les résultats de l'évaluation resteront inchangés jusqu'à ce que la règle soit supprimée, ce qui peut entraîner une augmentation inattendue de la création de CI `AWS::Config::ResourceCompliance` lors de la suppression de la règle.

Pour plus d'informations sur la façon de définir AWS Config des règles Lambda personnalisées `NOT_APPLICABLE` pour récupérer les ressources supprimées, voir Gestion des ressources supprimées à l'aide de règles Lambda AWS Config personnalisées.

Recommandation : fournir les ressources nécessaires pour les règles Lambda personnalisées

AWS Config Les règles Lambda personnalisées peuvent entraîner un nombre élevé d'appels de fonctions Lambda si la règle n'est pas limitée à un ou plusieurs types de ressources. Pour éviter une augmentation de l'activité associée à votre compte, il est vivement recommandé de fournir des ressources correspondant à vos règles Lambda personnalisées. Si aucun type de ressource n'est sélectionné, la règle invoquera la fonction Lambda pour toutes les ressources du compte.

Prise en charge de la région

Actuellement, la fonctionnalité AWS Config Règle est prise en charge dans les AWS régions suivantes. Pour obtenir une liste des AWS Config règles individuelles prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Nom de la région	Région	Point de terminaison	Protocole	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
		config-fips.us-east-2.amazonaws.com	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
Afrique (Le Cap)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asie-Pacifique (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada Ouest (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Espagne)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israël (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Moyen-Orient (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Le déploiement de AWS Config règles sur les comptes des membres d'une AWS organisation est pris en charge dans les régions suivantes.

Nom de la région	Région	Point de terminaison	Protocole
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Composantes d'une AWS Config règle

AWS Config les règles évaluent les paramètres de configuration de vos AWS ressources. Il existe deux types de règles : les règles gérées AWS Config et les règles personnalisées AWS Config .

AWS Config Les règles gérées sont des règles prédéfinies et personnalisables créées par AWS Config. Pour obtenir la liste des règles gérées, consultez la section Liste des règles AWS Config gérées.

AWS Config Les règles personnalisées sont des règles que vous créez de toutes pièces. Il existe deux manières de créer des règles AWS Config personnalisées : avec les fonctions Lambda (Guide du AWS Lambda développeur) et avec Guard (Guard GitHub Repository), un policy-as-code langage. AWS Config les règles personnalisées créées avec AWS Lambda sont appelées règles Lambda AWS Config personnalisées et les règles AWS Config personnalisées créées avec Guard sont appelées règles de politique AWS Config personnalisées.

Cette page décrit les métadonnées des règles AWS Config gérées et les meilleures pratiques sur la façon d'écrire des règles AWS Config personnalisées avec Python à l'aide du kit de développement de AWS Config règles (RDK) et de la bibliothèque de kits de développement de AWS Config règles (RDKlib).

Pour une présentation expliquant comment créer des règles de stratégie AWS Config personnalisées, consultez la section Création de règles de politique AWS Config personnalisées. Pour une présentation expliquant comment créer des règles Lambda AWS Config personnalisées, voir Création de règles Lambda AWS Config personnalisées.

Table des matières

- AWS Config métadonnées de règles gérées
- AWS Config structure de règles personnalisée
  - Écriture de règles
  - Logique de règles

AWS Config métadonnées de règles gérées

AWS Config les règles gérées peuvent contenir les métadonnées modifiables suivantes :

defaultName

Le defaultName est le nom que les instances d'une règle recevront par défaut.

description

La description de la règle fournit le contexte de ce que la règle évalue. Une limite de 256 caractères est appliquée à la console AWS Config . En vertu des bonnes pratiques, la description de la règle doit commencer par « Vérifie si » et inclure une description du scénario NON_COMPLIANT. Les noms de service doivent être écrits en entier, en commençant par AWS ou Amazon lorsqu'ils sont mentionnés pour la première fois dans la description de la règle. Par exemple, AWS CloudTrail ou Amazon CloudWatch au lieu de CloudTrail ou CloudWatch pour la première utilisation. Les noms des services peuvent être abrégés après référence ultérieure.

scope

La portée détermine les types de ressources ciblés par la règle. Pour obtenir la liste des types de ressources pris en charge, consultez Types de ressources pris en charge.

InputParameterInformations obligatoires

Les compulsoryInputParameter détails sont utilisés pour les paramètres nécessaires à l'évaluation d'une règle. Par exemple, la règle `access-keys-rotated` gérée inclut le paramètre requis `maxAccessKeyAge`. Si un paramètre est obligatoire, il ne sera pas marqué (facultatif). Un type doit être spécifié pour chaque paramètre. Le type peut être « String », « int », « double », « CSV », « boolean » ou « ». StringMap

InputParameterDétails facultatifs

Les optionalInputParameter détails sont utilisés pour les paramètres facultatifs permettant à une règle de procéder à son évaluation. Par exemple, la règle `elasticsearch-logs-to-cloudwatch` gérée inclut le paramètre facultatif `logTypes`. Un type doit être spécifié pour chaque paramètre. Le type peut être « String », « int », « double », « CSV », « boolean » ou « ». StringMap

pris en charge EvaluationModes

Il supportedEvaluationModes détermine le moment où les ressources seront évaluées, soit avant qu'une ressource soit déployée, soit après le déploiement d'une ressource.

`DETECTIVE` est utilisé pour évaluer les ressources déjà déployées. Vous pouvez ainsi évaluer les paramètres de configuration de vos ressources existantes. `PROACTIVE` est utilisé pour évaluer les ressources avant leur déploiement.

Cela vous permet d'évaluer si un ensemble de propriétés de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région.

Vous pouvez spécifier le supportedEvaluationModes to `DETECTIVEPROACTIVE`, ou les deux `DETECTIVE` et`PROACTIVE`. Vous devez spécifier un mode d'évaluation et ce champ ne peut pas rester vide.

Pour plus d'informations, consultez Modes d'évaluation. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

AWS Config structure de règles personnalisée

Cette section contient des informations sur l'utilisation du kit de développement de AWS Config règles (RDK) et de la bibliothèque de kits de développement de AWS Config règles (RDKlib). Pour plus d'informations sur le RDK ou RDKlib, consultez les référentiels aws-config-rdk et aws-config-rdklib. GitHub

Écriture de règles

Prérequis

1. Suivez les étapes décrites dans Installation de l' AWS CLI.
2. Suivez les étapes décrites dans Configuration à l' AWS Config aide de la console ou Configuration à l' AWS Config aide du AWS CLI. Pour plus d'informations sur les AWS régions AWS Config prises en charge, sélectionnez votre région dans la liste des services AWS régionaux.
3. Installez le kit RDK en utilisant la méthode recommandée avec pip :

```
pip install rdk
```

> **Note**
>
> Avant d'utiliser pip, vérifiez qu'il est installé sur votre ordinateur.

4. Installez la bibliothèque RDKLib en utilisant la méthode recommandée avec pip :

```
pip install rdklib
```

> **Note**
>
> Avant d'utiliser pip, vérifiez qu'il est installé sur votre ordinateur.

Règles déclenchées par des modifications

1. Pour créer une règle déclenchée par une modification du type de ressource spécifié, exécutez la commande suivante :

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type
```

L'exemple suivant crée une règle déclenchée par une modification du type de ressource `AWS::IAM::User` :

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
```

Voici les indicateurs que vous pouvez utiliser avec la commande `rdk create` pour les règles déclenchées par des modifications :

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

> **Note**
>
> Pour utiliser la bibliothèque RDKLib, l'exécution de la règle doit être définie sur `python3.6-lib`.

Après l'exécution de `rdk create`, vous devriez voir un nouveau répertoire portant le nom de la règle et contenant 3 fichiers :

- *RULE_NAME*`.py` : fichier Python contenant la logique de la règle
- *RULE_NAME*`_test.py` : fichier Python contenant les tests unitaires de la règle
- `parameters.json` : fichier JSON contenant les paramètres de déploiement du kit RDK

2. L'étape suivante consiste à écrire la logique de la règle. Il vous suffira de modifier le fichier *RULE_NAME*.py. Si vous ouvrez le fichier *RULE_NAME*.py, vous accéderez à un modèle vous permettant d'ajouter la logique de la règle. Le modèle suivant a été généré pour MFA_ENABLED_RULE :

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

##############################
```

```
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

L'exemple suivant est une version modifiée du modèle MFA_ENABLED_RULE avec la logique de la règle. La règle vérifie si l'authentification multifactorielle (MFA) est activée pour les utilisateurs IAM. La règle est NON_COMPLIANT si la MFA n'est pas activée pour un utilisateur IAM. Pour plus d'informations sur la logique des règles et les méthodes fournies dans le modèle, consultez Logique de règles.

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):

        username = configuration_item.get("resourceName")

        iam_client = client_factory.build_client("iam")

        response = iam_client.list_mfa_devices(UserName=username)

        # Scenario:1 IAM user has MFA enabled.
        if response["MFADevices"]:
            return [Evaluation(ComplianceType.COMPLIANT)]

        # Scenario:2 IAM user has MFA not enabled.
        annotation = "MFA needs to be enabled for user."
        return [Evaluation(ComplianceType.NON_COMPLIANT, annotation=annotation)]

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
```

```
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. L'étape suivante consiste à installer la couche RDKLib AWS avec la AWS console ou. AWS CLI RDKLib est conçue pour fonctionner en tant que couche AWS Lambda . Cela vous permet d'utiliser la bibliothèque sans l'ajouter à votre package de déploiement.

   - Pour installer la couche RDKLib avec la AWS console, procédez comme suit :

     1. Ouvrez la AWS Serverless Application Repository console à l'adresse https://console.aws.amazon.com/serverlessrepo.
     2. Dans le menu de navigation de gauche, sélectionnez Applications disponibles.
     3. Recherchez `rdklib` et choisissez rdklib.
     4. Examinez les détails de la fonction, puis déployez-la. Aucune modification ne devrait être nécessaire.
     5. Dans la section Ressources de la page de présentation, copiez le nom de ressource Amazon (ARN) de la couche Lambda. L'ARN de la couche Lambda sera nécessaire pour déployer votre règle.

   - Pour installer la couche RDKLib avec le AWS CLI, exécutez les commandes suivantes :

     1. Créez le jeu de modifications pour la couche RDKlib.

        ```
        aws serverlessrepo create-cloud-formation-change-set --application-id
         arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
        stack-name RDKlib-Layer
        ```

        La sortie suivante est renvoyée :

        ```
        {
            "ApplicationId": "arn:aws:serverlessrepo:ap-
        southeast-1:711761543063:applications/rdklib",
            "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
        a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
            "SemanticVersion": "0.1.0",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
        serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
        }
        ```

2. Exécutez le jeu de modifications. Vous pouvez copier/coller l'ARN complet du change-set ChangeSetId (à partir de la sortie générée à l'étape précédente) pour personnaliser la commande suivante :

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. Renvoie toutes les ressources associées qui font partie de la pile déployée.

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

La sortie suivante est renvoyée :

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. Copiez l'ARN de la couche Lambda provenant de la sortie générée à l'étape précédente. L'ARN de la couche Lambda est le `PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. L'étape suivante consiste à attribuer un rôle à la fonction Lambda. Par défaut, les fonctions Lambda tentent d'assumer le rôle `AWSServiceRoleForConfig`, ce qui n'est pas autorisé. Vous devez créer un rôle avec la politique `AWS_ConfigRole` gérée. Le rôle doit entretenir une

relation d'approbation avec AWS Config . Tous les rôles situés sous le chemin /rdk/ doivent assumer le rôle. Voici un exemple de politique d'approbation :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

Exécutez la commande suivante à l'aide de cette politique d'approbation :

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

Exécutez la commande suivante pour mettre à jour le paramètre d'entrée pour `ExecutionRoleName` et fournir le nom du rôle :

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-
name"}'
```

Vous pouvez également utiliser `rdk modify` pour mettre à jour les détails des règles déclenchées par des modifications à l'aide des indicateurs suivants :

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

5. La dernière étape consiste à déployer votre règle. Pour déployer votre règle, exécutez la commande suivante avec l'ARN de la couche Lambda mentionné à l'étape 3 :

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. La règle est désormais déployée. Vous pouvez utiliser la AWS Config console pour vérifier si la règle fonctionne comme prévu.

Règles périodiques

1. Pour créer une règle déclenchée périodiquement pour un type de ressource spécifié, exécutez la commande suivante :

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type --maximum-frequency EXECUTION_FREQUENCY
```

L'exemple suivant crée une règle déclenchée toutes les 24 heures pour le type de ressource `AWS::IAM::User` :

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
 --maximum-frequency TwentyFour_Hours
```

Voici les indicateurs que vous pouvez utiliser avec la commande `rdk create` pour les règles périodiques :

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

```
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

> **Note**
>
> Pour utiliser la bibliothèque RDKLib, l'exécution de la règle doit être définie sur `python3.6-lib`.

Après l'exécution de `rdk create`, vous devriez voir un nouveau répertoire portant le nom de la règle et contenant 3 fichiers :

- *RULE_NAME*`.py` : fichier Python contenant la logique de la règle
- *RULE_NAME*`_test.py` : fichier Python contenant les tests unitaires de la règle
- `parameters.json` : fichier JSON contenant les paramètres de déploiement du kit RDK

2. L'étape suivante consiste à écrire la logique de la règle. Il vous suffira de modifier le fichier *RULE_NAME*.py. Si vous ouvrez le fichier *RULE_NAME*.py, vous accéderez à un modèle vous permettant d'ajouter la logique de la règle. Le modèle suivant a été généré pour MFA_ENABLED_RULE :

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
```

```
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

Le modèle utilise par défaut les règles déclenchées par des modifications. Ajoutez plutôt votre logique à la méthode `evaluate_periodic`. L'exemple suivant est une version modifiée du modèle MFA_ENABLED_RULE avec la logique de la règle. La règle vérifie si l'authentification multifactorielle (MFA) est activée pour les utilisateurs IAM. La règle est NON_COMPLIANT si la MFA n'est pas activée pour un utilisateur IAM. Pour plus d'informations sur la logique des règles et les méthodes fournies dans le modèle, consultez Logique de règles.

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):l

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        evaluations = []

        iam_client = client_factory.build_client("iam")

        paginator = iam_client.get_paginator("list_users")
        response_iterator = paginator.paginate()

        for response in response_iterator:
            for user in response["Users"]:
                username = user["UserName"]
                response = iam_client.list_mfa_devices(UserName=username)

                # Scenario:1 IAM user has MFA enabled.
                if response["MFADevices"]:
                    evaluations.append(Evaluation(ComplianceType.COMPLIANT,
 username, "AWS::IAM::User"))

                # Scenario:2 IAM user has MFA not enabled.
```

```
                if not response["MFADevices"]:
                    annotation = "MFA needs to be enabled for user."
                    evaluations.append(
                        Evaluation(ComplianceType.NON_COMPLIANT, username,
 "AWS::IAM::User", annotation=annotation)
                    )
        return evaluations

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. L'étape suivante consiste à installer la couche RDKLib AWS avec la AWS console ou. AWS CLI RDKLib est conçue pour fonctionner en tant que couche AWS Lambda . Cela vous permet d'utiliser la bibliothèque sans l'ajouter à votre package de déploiement.

   - Pour installer la couche RDKLib avec la AWS console, procédez comme suit :

     1. Ouvrez la AWS Serverless Application Repository console à l'adresse https://console.aws.amazon.com/serverlessrepo.
     2. Dans le menu de navigation de gauche, sélectionnez Applications disponibles.
     3. Recherchez `rdklib` et choisissez rdklib.
     4. Examinez les détails de la fonction, puis déployez-la. Aucune modification ne devrait être nécessaire.
     5. Dans la section Ressources de la page de présentation, copiez le nom de ressource Amazon (ARN) de la couche Lambda. L'ARN de la couche Lambda sera nécessaire pour déployer votre règle.

   - Pour installer la couche RDKLib avec le AWS CLI, exécutez les commandes suivantes :

     1. Créez le jeu de modifications pour la couche RDKlib.

```
aws serverlessrepo create-cloud-formation-change-set --application-id
 arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
stack-name RDKlib-Layer
```

La sortie suivante est renvoyée :

```
{
    "ApplicationId": "arn:aws:serverlessrepo:ap-
southeast-1:711761543063:applications/rdklib",
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
    "SemanticVersion": "0.1.0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
}
```

2. Exécutez le jeu de modifications. Vous pouvez copier/coller l'ARN complet du change-set ChangeSetId (à partir de la sortie générée à l'étape précédente) pour personnaliser la commande suivante :

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. Renvoie toutes les ressources associées qui font partie de la pile déployée.

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

La sortie suivante est renvoyée :

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
```

```
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. Copiez l'ARN de la couche Lambda provenant de la sortie générée à l'étape précédente. L'ARN de la couche Lambda est le `PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. L'étape suivante consiste à attribuer un rôle à la fonction Lambda. Par défaut, les fonctions Lambda tentent d'assumer le rôle `AWSServiceRoleForConfig`, ce qui n'est pas autorisé. Vous devez créer un rôle avec la politique `AWS_ConfigRole` gérée. Le rôle doit entretenir une relation d'approbation avec AWS Config . Tous les rôles situés sous le chemin /rdk/ doivent assumer le rôle. Voici un exemple de politique d'approbation :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
```

```
  ]
}
```

Exécutez la commande suivante à l'aide de cette politique d'approbation :

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

Exécutez la commande suivante pour mettre à jour le paramètre d'entrée pour `ExecutionRoleName` et fournir le nom du rôle :

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-
name"}'
```

Vous pouvez également utiliser `rdk modify` pour mettre à jour les détails des règles périodiques à l'aide des indicateurs suivants :

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

5. La dernière étape consiste à déployer votre règle. Pour déployer votre règle, exécutez la commande suivante avec l'ARN de la couche Lambda mentionné à l'étape 3 :

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. La règle est désormais déployée. Vous pouvez utiliser la AWS Config console pour vérifier si la règle fonctionne comme prévu.

Logique de règles

L'exemple de code Python suivant est un modèle dédié à l'écriture d'une règle à l'aide du kit RDK et de la bibliothèque RDKLib. Vous ne devez apporter des modifications qu'aux méthodes

`evaluate_parameters`, `evaluate_change` et `evaluate_periodic`, ou écrire des nouvelles fonctions pour simplifier la logique si nécessaire. Pour connaître les conditions préalables à l'écriture des règles avec le kit RDK et la bibliothèque RDKLib, consultez Prérequis.

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ["AWS::Resource::Type"]

# When you create a rule, the class name will be the name you give the rule when you
 create it instead of ConfigRule
class ConfigRule (ConfigRule):

    def evaluate_parameters(self, rule_parameters):
        return rule_parameters

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ###############################
        # Add your custom logic here. #
        ###############################

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        ###############################
        # Add your custom logic here. #
        ###############################

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = ConfigRule()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

APPLICABLE_RESOURCES

`APPLICABLE_RESOURCES` sont le ou les types de ressources ciblés par la règle. S'ils sont utilisés, il doit s'agir d'une variable globale définie sur le ou les types de ressources ciblés par la règle. Pour obtenir la liste des types de ressources pris en charge, consultez Types de ressources pris en charge.

evaluate_parameters

Description

Cette méthode est utilisée pour vérifier si les paramètres d'entrée de la règle sont valides. Voici les bonnes pratiques associées :

- Vérifier si le nombre correct de paramètres est répertorié.
- Vérifier si le nom du paramètre est correct.
- Vérifier si la valeur du paramètre présente le type approprié.
- Si le paramètre est un entier, vérifier s'il se situe dans des limites raisonnables.
- Si le nombre d'options possibles pour le paramètre est limité, vérifier si le paramètre correspond à l'une de ces options.
- Si le paramètre est une chaîne, vérifier si sa longueur est raisonnable et supprimer tout espace avant ou après la valeur.
- Vérifier si la sensibilité à la casse est traitée de manière appropriée.
- Limiter si possible la saisie des paramètres. Si vous recevez par exemple une liste d'ARN séparés par des virgules, assurez-vous que les seuls caractères autorisés sont les virgules et les caractères pris en charge par les ARN.

Paramètres

`rule_parameters` est un dictionnaire des paramètres d'entrée de la règle.

Syntaxe de retour

Si l'un des paramètres n'est pas valide, vous pouvez générer une erreur `InvalidParametersError` :

```
from rdklib import InvalidParametersError
raise InvalidParametersError("Error message to display")
```

Si les paramètres sont tous valides, la méthode doit renvoyer un dictionnaire :

```
return valid_rule_parameters
```

evaluate_change

Description

Cette méthode est utilisée pour la logique d'évaluation d'une règle déclenchée par des modifications.

Paramètres

`event`est l' AWS Lambda événement proposé par AWS Config. Il s'agit d'un document au format JSON qui contient les données nécessaires à l'exécution d'une fonction Lambda. Pour des exemples, voir Exemples d'événements pour AWS Config les règles.

`client_factory`est l' ClientFactory objet à utiliser pour la règle. La ClientFactory classe crée ou réutilise un client boto3, qui fournit une interface de bas niveau à un service. AWS Les méthodes du client boto3 sont mappées à une API de AWS service, ce qui signifie que les opérations de service sont mappées aux méthodes client du même nom et donnent accès aux mêmes paramètres d'opération. Pour une liste des services disponibles, consultez Services disponibles dans la documentation Boto3 Docs.

La syntaxe de demande de `client_factory` est la suivante :

```
response = client_factory.build_client(
    service='string')
```

Par exemple :

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> Le nom boto3 du AWS service est obligatoire.

`configuration_item` est le dictionnaire de l'élément de configuration complet, même s'il est surdimensionné. Un élément de configuration représente une point-in-time vue des différents attributs d'une AWS ressource prise en charge. Pour plus d'informations sur le contenu de`ConfigurationItem`, reportez-vous ConfigurationItemà la référence de l' AWS Config API.

`valid_rule_parameters` est la sortie de la méthode `evaluate_parameters()`.

Syntaxe de retour

La méthode doit renvoyer un ou plusieurs des éléments suivants :

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> Les règles signalant les ressources supprimées doivent renvoyer le résultat de l'évaluation `NOT_APPLICABLE` afin d'éviter des évaluations de règles inutiles.

Vous devez utiliser des annotations pour toutes les évaluations non conformes. Par exemple :

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

evaluate_periodic

Description

Cette méthode est utilisée pour évaluer une règle périodique.

Paramètres

`event`est l' AWS Lambda événement proposé par AWS Config. Il s'agit d'un document au format JSON qui contient les données nécessaires à l'exécution d'une fonction Lambda. Pour des exemples, voir Exemples d'événements pour AWS Config les règles.

`client_factory`est l' ClientFactory objet à utiliser pour la règle. La ClientFactory classe crée ou réutilise un client boto3, qui fournit une interface de bas niveau à un service. AWS Les méthodes du client boto3 sont mappées à une API de AWS service, ce qui signifie que les opérations de service sont mappées aux méthodes client du même nom et donnent accès aux mêmes paramètres d'opération. Pour une liste des services disponibles, consultez Services disponibles dans la documentation Boto3 Docs.

La syntaxe de demande de `client_factory` est la suivante :

```
response = client_factory.build_client(
```

```
    service='string')
```

Par exemple :

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> Le nom boto3 du AWS service est obligatoire.

`valid_rule_parameters` est la sortie de la méthode `evaluate_parameters()`.

Syntaxe de retour

La méthode doit renvoyer un ou plusieurs des éléments suivants :

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> Les règles signalant les ressources supprimées doivent renvoyer le résultat de l'évaluation `NOT_APPLICABLE` afin d'éviter des évaluations de règles inutiles.

Vous devez utiliser des annotations pour toutes les évaluations non conformes. Par exemple :

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

lambda_handler

Description

Il ne devrait pas être nécessaire de modifier cette méthode. Le gestionnaire Lambda est utilisé pour traiter les événements. La fonction s'exécute lorsque AWS Lambda l'`event`objet est transmis à la `handler` méthode. Pour plus d'informations, consultez Gestionnaire de fonctions Lambda dans Python.

Paramètres

`event`est l' AWS Lambda événement proposé par AWS Config. Il s'agit d'un document au format JSON qui contient les données nécessaires à l'exécution d'une fonction Lambda. Pour des exemples, voir Exemples d'événements pour AWS Config les règles.

`context` est un objet transmis à votre fonction par Lambda au moment de l'exécution. Cet objet contient des méthodes et des propriétés qui fournissent des informations et des méthodes susceptibles d'être utilisées par la fonction pendant son exécution. Sachez que le contexte n'est plus utilisé dans les nouvelles versions de Lambda.

Mode d'évaluation et types de déclencheurs pour les AWS Config règles

Lorsque vous ajoutez une règle à votre compte, vous pouvez indiquer à quel moment du processus de création et de gestion des ressources vous AWS Config souhaitez évaluer vos ressources. Le processus de création et de gestion des ressources est connu sous le nom de mise en service des ressources. Vous choisissez le mode d'évaluation pour spécifier à quel moment vous souhaitez évaluer vos ressources AWS Config au cours de ce processus.

Selon la règle, AWS Config vous pouvez évaluer vos configurations de ressources avant le déploiement d'une ressource, après le déploiement d'une ressource, ou les deux. L'évaluation d'une ressource avant son déploiement est une évaluation proactive. L'évaluation d'une ressource après son déploiement est une évaluation détective.

Vous pouvez également choisir le type de déclencheur pour indiquer la fréquence à laquelle vous souhaitez que vos règles AWS Config évaluent vos ressources. Les ressources peuvent être évaluées lors de changements de configuration, selon un calendrier périodique, ou les deux.

Types de déclencheurs

Après avoir ajouté une règle à votre compte, AWS Config comparez vos ressources aux conditions de cette règle. Après cette évaluation initiale, AWS Config continue à exécuter des évaluations

chaque fois qu'une évaluation est déclenchée. Les déclencheurs d'évaluation sont définis dans le cadre de la règle et ils peuvent inclure les types suivants :

Type de déclencheur	Description
Configuration changes	AWS Config exécute des évaluations pour la règle lorsqu'une ressource correspond au champ d'application de la règle et qu'il y a un changement de configuration de la ressource. L'évaluation s'exécute après l' AWS Config envoi d'une notification de modification d'élément de configuration. Vous choisissez quelles ressources déclenche nt l'évaluation en définissant la portée de la règle. La portée peut inclure les éléments suivants : • Un ou plusieurs types de ressources • Une combinaison d'un type de ressource et d'un ID de ressource • Une combinaison d'une clé de balise et d'une valeur • Lorsqu'une ressource enregistrée est créée, mise à jour ou supprimée AWS Config exécute l'évaluation lorsqu'il détecte une modification apportée à une ressource correspondant au champ d'applica tion de la règle. Vous pouvez utiliser la portée afin de définir les ressources qui déclenchent des évaluations.
Périodique	AWS Config exécute des évaluations de la règle à la fréquence que vous choisissez, par exemple toutes les 24 heures.

Type de déclencheur	Description
Hybride	Certaines règles comportent à la fois des changements de configuration et des déclencheurs périodiques. Pour ces règles, AWS Config évalue vos ressources lorsqu'il détecte un changement de configuration et également à la fréquence que vous spécifiez.

Modes d'évaluation

Il existe deux modes d'évaluation :

Mode proactif

Utilisez l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriétés de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région.

Le schéma du type de ressource indique les propriétés d'une ressource. Vous pouvez trouver le schéma du type de ressource dans « extensions AWS publiques » du AWS CloudFormation registre ou à l'aide de la commande CLI suivante :

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Pour plus d'informations, consultez la section Gestion des extensions via le AWS CloudFormation registre et la référence aux types de AWS ressources et de propriétés dans le guide de AWS CloudFormation l'utilisateur.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Liste des règles gérées avec une évaluation proactive

Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.

Liste des types de ressources pris en charge pour une évaluation proactive

Voici une liste des types de ressources pris en charge pour une évaluation proactive :

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

Exemple de règle avec une évaluation proactive

Exemples de règles proactives

1. Vous ajoutez la règle AWS Config gérée`S3_BUCKET_LOGGING_ENABLED`, à votre compte pour vérifier si la journalisation est activée dans vos compartiments S3.
2. Pour le mode d'évaluation, choisissez Activer l'évaluation proactive dans la console de AWS gestion ou activer `PROACTIVE` `EvaluationModes` dans l'PutConfigRuleAPI.

Après avoir activé l'évaluation proactive, vous pouvez utiliser l'StartResourceEvaluationAPI et l'GetResourceEvaluationSummaryAPI pour vérifier si la journalisation n'est pas activée pour un bucket de votre compte, qui n'a pas été déployé en production. Vous pouvez ainsi tester les configurations des ressources avant de les déployer et réévaluer si vous souhaitez déployer la ressource concernée en production.

Par exemple, commencez par l' StartResourceEvaluation API :

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::S3::Bucket",
                                     "ResourceConfiguration": "{\"BucketName\": \"my-
bucket\", \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Vous devriez recevoir le `ResourceEvaluationId` dans la sortie :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Ensuite, utilisez l'API `ResourceEvaluationId` avec l' GetResourceEvaluationSummary API pour vérifier le résultat de l'évaluation :

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Votre résultat doit être similaire à ce qui suit :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration": "{\"BucketName\": \"my-bucket\",
 \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",
```

```
    }
}
```

Pour obtenir des informations supplémentaires sur le résultat de l'évaluation, telles que la règle qui a marqué une ressource comme NON_COMPLIANT, utilisez l'API. GetComplianceDetailsByResource

Mode détectif

Utilisez l'évaluation détective pour évaluer les ressources déjà déployées. Ce type d'évaluation vous permet d'évaluer les paramètres de configuration de vos ressources existantes.

Exemples de règles avec l'évaluation détective

Exemple de règle déclenchée par des modifications

1. Vous ajoutez la règle gérée, `S3_BUCKET_LOGGING_ENABLED`, à votre compte pour vérifier si la journalisation est activée pour les compartiments S3.
2. Le type de déclencheur de la règle est le changement de configuration. AWS Config exécute les évaluations de la règle lorsqu'un compartiment S3 est créé, modifié ou supprimé.
3. Lorsqu'un compartiment est mis à jour, le changement de configuration déclenche la règle et AWS Config évalue si le compartiment est conforme à la règle.

Exemples de règles périodiques

1. Vous ajoutez la règle gérée, `IAM_PASSWORD_POLICY`, à votre compte. La règle vérifie si la politique de mot de passe pour vos utilisateurs IAM est conforme à la politique de compte, par exemple si elle respecte la longueur minimale ou les caractères spécifiques nécessaires.
2. Le type de déclencheur de la règle est périodique. AWS Config exécute l'évaluation de la règle à une fréquence que vous spécifiez, par exemple toutes les 24 heures.
3. Toutes les 24 heures, la règle est initiée et AWS Config évalue si les mots de passe de vos utilisateurs IAM sont conformes à la règle.

Exemple de règle hybride avec changement de configuration et déclencheurs périodiques

1. Créez une règle personnalisée qui évalue si les AWS CloudTrail sentiers de votre compte sont activés et enregistrés pour toutes les régions.
2. Vous AWS Config souhaitez évaluer la règle chaque fois qu'un journal est créé, mis à jour ou supprimé. Vous souhaitez également AWS Config exécuter la règle toutes les 12 heures.

3. Concernant le type de déclencheur, vous écrivez une logique pour les changements de configuration et les déclencheurs périodiques. Pour plus d'informations, voir Composants d'une AWS Config règle : règles d'écriture.

Évaluations de règle lorsque l'enregistreur de configuration est désactivé

Si vous désactivez l'enregistreur de configuration, il AWS Config arrête d'enregistrer les modifications apportées à vos configurations de ressources. Cela affecte les évaluations de règle de la façon suivante :

- Les règles périodiques continuent d'exécuter des évaluations à la fréquence spécifiée.
- Les règles déclenchées par des modifications n'exécutent pas d'évaluations.
- Les règles hybrides exécutent les évaluations uniquement à la fréquence spécifiée. Les règles n'exécutent pas les évaluations pour les changements de configuration.
- Si vous exécutez une évaluation à la demande pour une règle avec déclencheur en cas de changement de configuration, la règle évalue le dernier état connu de la ressource, qui est le dernier élément de configuration enregistré.

> **Important**
>
> Évitez les AWS Config évaluations inutiles
>
> Les règles périodiques et les règles hybrides continueront de s'exécuter jusqu'à ce qu'elles soient supprimées, même si vous avez désactivé l'enregistreur de configuration. Ces règles évalueront uniquement les éléments de configuration enregistrés avant la désactivation de l'enregistreur de configuration. Par conséquent, elles reproduiront les mêmes résultats d'évaluation sans nouvelles informations. Supprimez les règles périodiques et les règles hybrides lorsque vous désactivez l'enregistreur de configuration afin d'éviter toute activité et toute évaluation de règles inutiles.

AWS Config Règles gérées

AWS Config fournit des règles AWS gérées, qui sont des règles prédéfinies et personnalisables AWS Config utilisées pour évaluer si vos AWS ressources sont conformes aux meilleures pratiques courantes. À titre d'exemple, vous pouvez utiliser une règle gérée pour commencer à évaluer rapidement si vos volumes Amazon Elastic Block Store (Amazon EBS) sont chiffrés ou si des

balises spécifiques s'appliquent à vos ressources. La AWS Config console vous guide tout au long du processus de configuration et d'activation d'une règle gérée. Vous pouvez également utiliser l' AWS Config API AWS Command Line Interface or pour transmettre le code JSON qui définit votre configuration d'une règle gérée.

Vous pouvez personnaliser le comportement d'une règle gérée en fonction de vos besoins. À titre d'exemple, vous pouvez définir l'étendue de la règle pour limiter les ressources qui déclenchent une évaluation de la règle, comme les volumes ou les instances EC2. Vous pouvez personnaliser les paramètres d'une règle pour définir les attributs dont vos ressources doivent disposer pour être conformes à la règle. Par exemple, vous pouvez personnaliser un paramètre pour spécifier que votre groupe de sécurité doit bloquer le trafic entrant d'un numéro de port spécifique.

Considérations de coût

Pour plus de détails sur les coûts associés à l'enregistrement des ressources, consultez la section AWS Config tarification.

Recommandation : arrêtez d'enregistrer la conformité des ressources avant de supprimer les règles

Il est vivement recommandé d'arrêter l'enregistrement pour le type de `AWS::Config::ResourceCompliance` ressource avant de supprimer les règles de votre compte. La suppression de règles crée des éléments de configuration (CI) pour votre enregistreur de configuration `AWS::Config::ResourceCompliance` et peut avoir une incidence sur les coûts AWS Config de votre enregistreur de configuration. Si vous supprimez des règles qui évaluent un grand nombre de types de ressources, cela peut entraîner une augmentation du nombre de CI enregistrés.

Bonnes pratiques :

1. Arrêter l'enregistrement `AWS::Config::ResourceCompliance`
2. Supprimer une ou plusieurs règles
3. Activez l'enregistrement pour `AWS::Config::ResourceCompliance`

Types de déclencheurs

Après avoir ajouté une règle à votre compte, AWS Config comparez vos ressources aux conditions de cette règle. Après cette évaluation initiale, AWS Config continue à exécuter des évaluations chaque fois qu'une évaluation est déclenchée. Les déclencheurs d'évaluation sont définis dans le cadre de la règle et peuvent inclure les types suivants.

Type de déclencheur	Description
Configuration changes	AWS Config exécute des évaluations pour la règle lorsqu'une ressource correspond au champ d'application de la règle et qu'il y a un changement de configuration de la ressource. L'évaluation s'exécute après l' AWS Config envoi d'une notification de modification d'élément de configuration. Vous choisissez quelles ressources déclenche nt l'évaluation en définissant la portée de la règle. La portée peut inclure les éléments suivants : • Un ou plusieurs types de ressources • Une combinaison d'un type de ressource et d'un ID de ressource • Une combinaison d'une clé de balise et d'une valeur • Lorsqu'une ressource enregistrée est créée, mise à jour ou supprimée AWS Config exécute l'évaluation lorsqu'il détecte une modification apportée à une ressource correspondant au champ d'applica tion de la règle. Vous pouvez utiliser la portée afin de définir les ressources qui déclenchent des évaluations.
Périodique	AWS Config exécute des évaluations de la règle à la fréquence que vous choisissez, par exemple toutes les 24 heures.

Type de déclencheur	Description
Hybride	Certaines règles comportent à la fois des changements de configuration et des déclencheurs périodiques. Pour ces règles, AWS Config évalue vos ressources lorsqu'il détecte un changement de configuration et également à la fréquence que vous spécifiez.

Modes d'évaluation

Il existe deux modes d'évaluation des AWS Config règles.

Mode d'évaluation	Description
Proactif	Utilisez l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriété s de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région. Pour plus d'informations, consultez Modes d'évaluation. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.
Détective	Utilisez l'évaluation détective pour évaluer les ressources déjà déployées. Ce type d'évaluat ion vous permet d'évaluer les paramètres de configuration de vos ressources existantes.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Rubriques

- Liste des règles AWS Config gérées
- Liste des règles AWS Config gérées par mode d'évaluation
- Liste des règles AWS Config gérées par type de déclencheur
- Liste des règles AWS Config gérées par région et disponibilité
- Règles liées aux services AWS Config
- Création de règles gérées AWS Config avec des modèles AWS CloudFormation

Liste des règles AWS Config gérées

AWS Config prend actuellement en charge les règles gérées suivantes.

Considérations

Valeurs par défaut pour les règles gérées

Les valeurs par défaut spécifiées pour les règles gérées sont préremplies uniquement lors de l'utilisation de la AWS console. Les valeurs par défaut ne sont pas fournies pour l'API, la CLI ou le kit SDK.

Les compartiments de répertoire ne sont pas pris en charge

Les règles gérées ne prennent en charge que les compartiments à usage général lors de l'évaluation des ressources Amazon Simple Storage Service (Amazon S3). AWS Config n'enregistre pas les modifications de configuration pour les compartiments de répertoire. Pour plus d'informations sur les compartiments à usage général et les compartiments de répertoires, consultez Présentation des compartiments et Compartiments de répertoires dans le Guide de l'utilisateur Amazon S3.

Règles gérées et types de ressources IAM globaux

Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que

AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Rubriques

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf

- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check

- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled

- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted

- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan

- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-s3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- vérification de l'expiration du certificat du serveur iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty

- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

access-keys-rotated

Vérifie si les clés d'accès actives font l'objet d'une rotation (modification) dans le temps imparti spécifié dans `maxAccessKeyAge`. La règle est NON_COMPLIANT si les clés d'accès n'ont pas fait l'objet d'une rotation dans le délai indiqué. La valeur par défaut est 90 jours.

> **Warning**
>
> Ne communiquez pas vos clés d'accès à des tiers non autorisés, même pour vous aider à trouver les identifiants de votre compte. En effet, vous lui accorderiez ainsi un accès permanent à votre compte. En matière de sécurité, les bonnes pratiques consistent à supprimer les mots de passe et les clés d'accès dont les utilisateurs n'ont plus besoin.

> **Note**
>
> Type de ressource marqué comme non conforme dans la console
> Si cette règle détecte que l'une de vos clés d'accès n'est pas conforme, le type de `AWS::IAM::User` ressource sera également marqué comme non conforme dans la AWS console.
> Règles gérées et types de ressources IAM globaux
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.
> Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez

pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.
Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.
Limites
Cette règle ne s'applique pas aux clés d'accès de l'utilisateur root du AWS compte.
Pour supprimer ou faire pivoter vos clés d'accès utilisateur root, utilisez vos informations d'identification d'utilisateur root pour vous connecter à la page Mes informations de sécurité dans le fichier AWS Management Console athttps://aws.amazon.com/console/.

Identificateur : ACCESS_KEYS_ROTATED

Types de ressources : AWS::IAM::User

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

AccessKeyâge maximum, Type : int, Valeur par défaut : 90

Nombre maximum de jours sans rotation. Valeur par défaut : 90.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

account-part-of-organizations

Vérifie si un AWS compte fait partie de AWS Organizations. La règle est NON_COMPLIANT si un AWS compte ne fait pas partie de AWS Organizations ou si l'ID du compte principal AWS d'Organizations ne correspond pas au paramètre de la règle. `MasterAccountId`

> **Note**
>
> Règles gérées et types de ressources IAM globaux

Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : ACCOUNT_PART_OF_ORGANIZATIONS

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

MasterAccountId (Facultatif), Type : chaîne

L'identifiant du compte principal d'un AWS compte.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

acm-certificate-expiration-check

Vérifie si les certificats AWS Certificate Manager de votre compte sont marqués pour expiration dans le nombre de jours spécifié. Les certificats fournis par ACM sont renouvelés automatiquement. ACM ne renouvelle pas les certificats que vous importez. La règle est NON_COMPLIANT si vos certificats sont sur le point d'expirer.

Identificateur : ACM_CERTIFICATE_EXPIRATION_CHECK

Types de ressources : AWS::ACM::Certificate

Type de déclencheur : modifications de configuration et périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

daysToExpiration (Facultatif), Type : int, Valeur par défaut : 14

Spécifiez le nombre de jours avant que la règle marque le certificat ACM comme étant non conforme.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

acm-certificate-rsa-check

Vérifie si les certificats RSA gérés par AWS Certificate Manager (ACM) ont une longueur de clé d'au moins « 2048 » bits. La règle est NON_COMPLIANT si la longueur de clé minimale est inférieure à 2048 bits.

Identificateur : ACM_CERTIFICATE_RSA_CHECK

Types de ressources : AWS::ACM::Certificate

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

acm-pca-root-ca-disabled

Vérifie si l'autorité de certification AWS AWS privée (autorité de certification privée) possède une autorité de certification racine désactivée. La règle est NON_COMPLIANT pour les autorités de certification racines dont le statut n'est pas DISABLED.

Identificateur : ACM_PCA_ROOT_CA_DISABLED

Types de ressources : AWS::ACMPCA::CertificateAuthority

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

exemptedCAArns (facultatif), Type : CSV

> Liste des Amazon Resource Name (ARN) séparés par des virgules des autorités de certification qui peuvent être activées. Cette valeur peut être fournie pour d'autres autorités de certification, telles que des autorités de certification racines spécifiques ou des autorités de certification intermédiaires pouvant être activées.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

alb-desync-mode-check

Vérifie si Application Load Balancer (ALB) est configuré avec un mode d'atténuation de désynchronisation défini par l'utilisateur. La règle est NON_COMPLIANT si le mode d'atténuation de désynchronisation ALB ne correspond pas au mode d'atténuation de désynchronisation défini par l'utilisateur.

Identificateur : ALB_DESYNC_MODE_CHECK

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

desyncMode, Type : CSV

Liste d'éléments séparés par des virgules, permettant aux clients de choisir au maximum 2 valeurs parmi : « défensif », « le plus strict » et « surveillance ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

alb-http-drop-invalid-header-enabled

Vérifie si la règle évalue les équilibreurs de charge d' AWS application (ALB) pour s'assurer qu'ils sont configurés pour supprimer les en-têtes HTTP. La règle est NON_COMPLIANT si la valeur de routing.http.drop_invalid_header_fields.enabled est définie sur false.

Identificateur : ALB_HTTP_DROP_INVALID_HEADER_ENABLED

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

alb-http-to-https-redirection-check

Vérifie si la redirection HTTP vers HTTPS est configurée sur tous les écouteurs HTTP d'Application Load Balancers. La règle est NON_COMPLIANT si la redirection HTTP vers HTTPS n'est pas configurée pour un ou plusieurs écouteurs HTTP d'Application Load Balancers. La règle est également NON_COMPLIANT si un ou plusieurs écouteurs HTTP sont acheminés vers un écouteur HTTP au lieu d'une redirection.

Identificateur : ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

alb-waf-enabled

Vérifie si le AWS WAF est activé sur les équilibreurs de charge d'application (ALB). La règle est NON_COMPLIANT si key: waf.enabled est défini sur false.

Identificateur : ALB_WAF_ENABLED

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

waf WebAclIds (facultatif), Type : CSV

Liste d'ID de listes ACL Web (pour WAF) ou d'ARN de listes ACL Web (pour WAFV2) séparés par des virgules vérifiant l'association ALB.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

api-gwv2-access-logs-enabled

Vérifie que la journalisation est activée pour les étapes V2 Amazon API Gateway. La règle est NON_COMPLIANT si « accès LogSettings » n'est pas présent dans la configuration de Stage.

Identificateur : API_GWV2_ACCESS_LOGS_ENABLED

Types de ressources : AWS::ApiGatewayV2::Stage

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

api-gwv2-authorization-type-configured

Vérifie si un type d'autorisation est défini pour les routes d'API Amazon API Gatewayv2. Cette règle est NON_COMPLIANT si le type d'autorisation est NONE.

Identificateur : API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

Types de ressources : AWS::ApiGatewayV2::Route

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

authorizationType (facultatif), Type : chaîne

> Paramètre permettant de vérifier les types d'autorisation des routes d'API. Les paramètres de chaîne correspondant à CUSTOM, AWS_IAM, JWT sont valides.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

api-gw-associated-with-waf

Vérifie si un stage d'API Amazon API Gateway utilise une liste de contrôle d'accès Web (ACL Web) AWS WAF. La règle est NON_COMPLIANT si aucune ACL Web AWS WAF n'est utilisée ou si une ACL AWS Web utilisée ne correspond pas à ce qui est indiqué dans le paramètre de règle.

Identificateur : API_GW_ASSOCIATED_WITH_WAF

Types de ressources : AWS::ApiGateway::Stage

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

WebAclArns (Facultatif), Type : CSV

Liste d'Amazon Resource Names (ARN) de listes ACL Web séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

api-gw-cache-enabled-and-encrypted

Vérifie si le cache est activé et chiffré pour toutes les méthodes des étapes Amazon API Gateway. La règle est NON_COMPLIANT si une méthode d'une étape Amazon API Gateway n'est pas configurée pour la mise en cache ou si le cache n'est pas chiffré.

Identificateur : API_GW_CACHE_ENABLED_AND_ENCRYPTED

Types de ressources : AWS::ApiGateway::Stage

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

api-gw-endpoint-type-check

Vérifie que les API Amazon API Gateway sont du type spécifié dans le paramètre de règle `endpointConfigurationType`. La règle renvoie NON_COMPLIANT si l'API REST ne correspond pas au type de point de terminaison configuré dans le paramètre de règle.

Identificateur : API_GW_ENDPOINT_TYPE_CHECK

Types de ressources : AWS::ApiGateway::RestApi

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

point final ConfigurationTypes, Type : chaîne

> Liste des autorisations séparées par des virgules. endpointConfigurationTypes Les valeurs autorisées sont REGIONAL, PRIVATE et EDGE.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

api-gw-execution-logging-enabled

Vérifie que la journalisation est activée pour toutes les méthodes des étapes Amazon API Gateway. La règle est NON_COMPLIANT si la journalisation n'est pas activée ou si `loggingLevel` n’est ni ERROR ni INFO.

Identificateur : API_GW_EXECUTION_LOGGING_ENABLED

Types de ressources : AWS::ApiGateway::Stage, AWS::ApiGateway V2 : :Stage

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

LoggingLevel (facultatif), Type : chaîne, Valeur par défaut : ERROR, INFO

> Liste de niveaux de journalisation spécifiques (par exemple, ERROR, INFO ou ERROR,INFO), séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

api-gw-ssl-enabled

Vérifie si une étape d'API REST utilise un certificat SSL. La règle est NON_COMPLIANT si l'étape de l'API REST n'est pas associée à un certificat SSL.

> **Note**
>
> Cette règle est renvoyée `NOT_APPLICABLE` si l'GetIntegrationAPI renvoie `AWS` en tant que type.

Identificateur : API_GW_SSL_ENABLED

Types de ressources : AWS::ApiGateway::Stage

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

CertificateIDs (facultatif), Type : CSV

Liste d'identifiants de certificats clients configurés sur une étape d'API REST, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

api-gw-xray-enabled

Vérifie si le suivi AWS X-Ray est activé sur les API REST d'Amazon API Gateway. La règle est COMPLIANT si le suivi X-ray est activé et NON_COMPLIANT dans le cas contraire.

Identificateur : API_GW_XRAY_ENABLED

Types de ressources : AWS::ApiGateway::Stage

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
```

```
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

approved-amis-by-id

Vérifie si les instances EC2 en cours d'exécution utilisent les Amazon Machine Images (AMI). Spécifiez une liste d'ID d'AMI approuvés. Les instances en cours d'exécution avec des AMI qui ne se trouvent pas sur cette liste sont NON_COMPLIANT.

Identificateur : APPROVED_AMIS_BY_ID

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

amiIds, Type : CSV

> Les ID d'AMI (liste contenant jusqu'à 21 ID d'AMI ou 1 024 caractères au total séparés par des virgules, selon la première éventualité).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

approved-amis-by-tag

Vérifie si les instances en cours d'exécution utilisent les Amazon Machine Images (AMI). Spécifiez les balises qui identifient les AMI. Les instances en cours d'exécution avec des AMI qui ne disposent pas d'au moins une des balises spécifiées sont NON_COMPLIANT.

Identificateur : APPROVED_AMIS_BY_TAG

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

ByTagKeyAndvaleur des amis, Type : StringMap, Valeur par défaut : tag-key:tag-value,other-tag-key

> Les AMI par balise (liste contenant jusqu'à 10 éléments séparés par des virgules ; par exemple, `tag-key:tag-value` ; c'est-à-dire que `tag-key1` correspond aux AMI avec `tag-key1`, `tag-key2:value2` correspond à `tag-key2`avec value2).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

appsync-associated-with-waf

Vérifie si les AWS AppSync API sont associées aux listes de contrôle d'accès Web (ACL) AWS WAFv2. La règle est NON_COMPLIANT pour une AWS AppSync API si elle n'est pas associée à une ACL Web.

Identificateur : APPSYNC_ASSOCIATED_WITH_WAF

Types de ressources : AWS::AppSync::Graph QLAPI

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

ARN waf (WebAclfacultatif), Type : CSV

> Liste d'Amazon Resource Names (ARN) séparés par des virgules pour les listes ACL Web autorisées.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

appsync-authorization-check

Vérifie si une AWS AppSync API utilise des mécanismes d'autorisation autorisés. La règle est NON_COMPLIANT si un mécanisme d'autorisation non approuvé est utilisé.

Identificateur : APPSYNC_AUTHORIZATION_CHECK

Types de ressources : AWS::AppSync::Graph QLAPI

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

AllowedAuthorizationLes types, Type : CSV

> Liste des mécanismes d' AWS AppSync autorisation autorisés séparés par des virgules. Les valeurs autorisées sont : « API_KEY », « AWS_LAMBDA », « AWS_IAM », « OPENID_CONNECT », « AMAZON_COGNITO_USER_POOLS ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

appsync-cache-encryption-at-rest

Vérifie si le chiffrement au repos est activé dans un cache d' AWS AppSync API. Cette règle est NON_COMPLIANT si « AtRest EncryptionEnabled » est faux.

Identificateur : APPSYNC_CACHE_ENCRYPTION_AT_REST

Types de ressources : AWS::AppSync::Graph QLAPI

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

appsync-logging-enabled

Vérifie si la journalisation est activée sur une AWS AppSync API. La règle est NON_COMPLIANT si la journalisation n'est pas activée ou si le champ LogLevel n'est ni ERROR ni ALL.

Identificateur : APPSYNC_LOGGING_ENABLED

Types de ressources : AWS::AppSync::Graph QLAPI

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

fieldLoggingLevel (Facultatif), Type : CSV

> Liste de niveaux de journalisation de champ spécifiques (par exemple, ERROR ou ALL), séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

athena-workgroup-encrypted-at-rest

Vérifie si un groupe de travail Amazon Athena est chiffré au repos. La règle est NON_COMPLIANT si le chiffrement des données au repos n'est pas activé pour un groupe de travail Athena.

Identificateur : ATHENA_WORKGROUP_ENCRYPTED_AT_REST

Types de ressources : AWS::Athena::WorkGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

aurora-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour les clusters de bases de données Amazon Aurora. La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans le cluster de bases de données Amazon Relational Database Service (Amazon RDS).

Identificateur : AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des clusters de bases de données Aurora pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du cluster de bases de données Aurora pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

aurora-meets-restore-time-target

Vérifie si la durée de restauration des clusters de base de données Amazon Aurora correspond à la durée spécifiée. La règle est NON_COMPLIANT si LatestRestoreExecutionTimeMinutes la durée d'un cluster de base de données Aurora est supérieure maxRestoreTime à quelques minutes.

Identifiant : AURORA_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balises des clusters de bases de données Aurora pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

ID du cluster de bases de données Aurora pour la règle à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

aurora-mysql-backtracking-enabled

Vérifie si le retour sur trace est activé sur un cluster Amazon Aurora MySQL. La règle est NON_COMPLIANT si le cluster Aurora utilise MySQL et si le retour sur trace n'est pas activé.

Identificateur : AURORA_MYSQL_BACKTRACKING_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Disponible uniquement en Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Sydney), Canada (Centre), Chine (Ningxia), Europe (Zurich) Région

Paramètres :

BacktrackWindowInHours (Facultatif), Type : double

> Délai exprimé en heures (jusqu'à 72) nécessaire pour appliquer le retour sur trace à votre cluster Aurora MySQL.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

aurora-resources-protected-by-backup-plan

Vérifie si les clusters de bases de données Amazon Aurora sont protégés par un plan de sauvegarde. La règle est NON_COMPLIANT si le cluster de bases de données Amazon Relational Database Service (Amazon RDS) n'est pas protégé par un plan de sauvegarde.

Identificateur : AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des clusters de bases de données Aurora pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du cluster de bases de données Aurora pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

autoscaling-capacity-rebalancing

Vérifie si le rééquilibrage de capacité est activé pour les groupes Amazon EC2 Auto Scaling qui utilisent plusieurs types d'instances. La règle est NON_COMPLIANT si le rééquilibrage de capacité n'est pas activé.

Identificateur : AUTOSCALING_CAPACITY_REBALANCING

Types de ressources : AWS::AutoScaling::AutoScaling Groupe

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

autoscaling-group-elb-healthcheck-required

Vérifie si vos groupes Amazon EC2 Auto Scaling associés à un Elastic Load Balancer utilisent les tests de santé d'Elastic Load Balancing. La règle est NON_COMPLIANT si les groupes Amazon EC2 Auto Scaling n'utilisent pas la surveillance de l'état Elastic Load Balancing.

Identificateur : AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Types de ressources : AWS::AutoScaling::AutoScaling Groupe

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*Les valeurs valides sont `EC2` (par défaut), `ELB` et `VPC_LATTICE`. Le type de surveillance de l'état `VPC_LATTICE` est réservé à l'utilisation de VPC Lattice, proposé en version préliminaire et susceptible d'être modifié. Pour plus d'informations, consultez Surveillance de l'état pour les instances Auto Scaling dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

autoscaling-launchconfig-requires-imdsv2

Vérifie si seul IMDSv2 est activé. Cette règle est NON_COMPLIANT si la version des métadonnées n'est pas incluse dans la configuration de lancement ou si les métadonnées V1 et V2 sont activées.

Identificateur : AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

Types de ressources : AWS::AutoScaling::LaunchConfiguration

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

autoscaling-launch-config-hop-limit

Vérifie le nombre de saut de réseau à réseau que le jeton de métadonnées peut effectuer. Cette règle est NON_COMPLIANT si la limite de sauts de réponse des métadonnées est supérieure à 1.

Identificateur : AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

Types de ressources : AWS::AutoScaling::LaunchConfiguration

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

autoscaling-launch-config-public-ip-disabled

Vérifie si les adresses IP publiques sont activées dans les groupes Amazon EC2 Auto Scaling via les configurations de lancement. La règle est NON_COMPLIANT si la configuration de lancement d'un AssociatePublicIpAddress groupe Amazon EC2 Auto Scaling est définie sur « true ».

Identificateur : AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

Types de ressources : AWS::AutoScaling::LaunchConfiguration

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

autoscaling-launch-template

Vérifie si un groupe Auto Scaling Amazon Elastic Compute Cloud (EC2) est créé à partir d'un modèle de lancement EC2. La règle est NON_COMPLIANT si aucun groupe de mise à l'échelle n'est créé à partir d'un modèle de lancement EC2.

Identificateur : AUTOSCALING_LAUNCH_TEMPLATE

Types de ressources : AWS::AutoScaling::AutoScaling Groupe

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

autoscaling-multiple-az

Vérifie si le groupe Auto Scaling couvre plusieurs zones de disponibilité. La règle est NON_COMPLIANT si le groupe Auto Scaling ne couvre pas plusieurs zones de disponibilité.

Identificateur : AUTOSCALING_MULTIPLE_AZ

Types de ressources : AWS::AutoScaling::AutoScaling Groupe

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

minAvailabilityZones (Facultatif), Type : int

Nombre minimum de zones de disponibilité attendues.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

autoscaling-multiple-instance-types

Vérifie si un groupe Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) utilise plusieurs types d'instances. Cette règle est NON_COMPLIANT si un seul type d'instance est défini pour le groupe Amazon EC2 Auto Scaling.

Identificateur : AUTOSCALING_MULTIPLE_INSTANCE_TYPES

Types de ressources : AWS::AutoScaling::AutoScaling Groupe

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

backup-plan-min-frequency-and-min-retention-check

Vérifie si un plan de sauvegarde présente une règle de sauvegarde qui satisfait à la fréquence et à la période de conservation requises. La règle est NON_COMPLIANT si la création des points de récupération est inférieure à la fréquence spécifiée ou s'ils expirent avant la période spécifiée.

Identificateur : BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

Types de ressources : AWS::Backup::BackupPlan

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

requiredFrequencyValue (Facultatif), Type : int, Valeur par défaut : 1

Valeur numérique correspondant à la fréquence de sauvegarde requise. Valeurs maximales : 24 pour les heures, 31 pour les jours.

requiredRetentionDays (Facultatif), Type : int, Valeur par défaut : 35

La période de conservation, en jours.

requiredFrequencyUnit (Facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à la fréquence de sauvegarde requise. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

backup-recovery-point-encrypted

Vérifie si un point de récupération est chiffré. La règle est NON_COMPLIANT si le point de récupération n'est pas chiffré.

Identificateur : BACKUP_RECOVERY_POINT_ENCRYPTED

Types de ressources : AWS::Backup::RecoveryPoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

backup-recovery-point-manual-deletion-disabled

Vérifie si un coffre-fort de sauvegarde est associé à une politique basée sur les ressources qui empêche la suppression des points de récupération. La règle est NON_COMPLIED si le Backup Vault ne dispose pas de politiques basées sur les ressources ou dispose de politiques dépourvues d'une instruction « Deny » appropriée (instruction avec autorisations backup : DeleteRecovery Point, backup : UpdateRecovery PointLifecycle et backup :). PutBackupVaultAccessPolicy

Identificateur : BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

Types de ressources : AWS::Backup::BackupVault

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

principalArnList (Facultatif), Type : CSV

> Liste séparée par des virgules des noms de ressources Amazon (ARN) AWS Identity and Access Management (IAM) (IAM) que la règle ne doit PAS vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

backup-recovery-point-minimum-retention-check

Vérifie si un point de récupération expire au plus tôt après la période spécifiée. La règle est NON_COMPLIANT si le point de récupération présente un point de rétention inférieur à la période de conservation requise.

Identificateur : BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

Types de ressources : AWS::Backup::RecoveryPoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

requiredRetentionDays (Facultatif), Type : int, Valeur par défaut : 35

La période de conservation, en jours.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

beanstalk-enhanced-health-reporting-enabled

Vérifie si un environnement AWS Elastic Beanstalk est configuré pour améliorer les rapports de santé. La règle est COMPLIANT si des rapports d'intégrité améliorés sont configurés dans l'environnement. La règle est NON_COMPLIANT si des rapports d'intégrité basiques sont configurés dans l'environnement.

Identificateur : BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

Types de ressources : AWS::ElasticBeanstalk::Environment

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

clb-desync-mode-check

Vérifie si des Classic Load Balancers (CLB) sont configurés avec un mode d'atténuation de désynchronisation défini par l'utilisateur. La règle est NON_COMPLIANT si le mode d'atténuation de désynchronisation CLB ne correspond pas au mode d'atténuation de désynchronisation défini par l'utilisateur.

Identificateur : CLB_DESYNC_MODE_CHECK

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

desyncMode, Type : CSV

> Liste de valeurs séparées par des virgules. Vous pouvez en sélectionner deux au maximum. Les valeurs valides sont « Defensive », « Strictest » et « Monitor ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

clb-multiple-az

Vérifie si un Classic Load Balancer couvre plusieurs zones de disponibilité (AZ). La règle est NON_COMPLIANT si un Classic Load Balancer couvre moins de 2 AZ ou s'il ne couvre pas le nombre d'AZ mentionnés dans le paramètre `minAvailabilityZones` (le cas échéant).

Identificateur : CLB_MULTIPLE_AZ

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

minAvailabilityZones (Facultatif), Type : int

Nombre minimum souhaité d'AZ attendues. Les valeurs valides sont comprises entre 2 et 10, les deux inclus. La valeur par défaut est 2 si aucune valeur n'est spécifiée.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

cloudformation-stack-drift-detection-check

Vérifie si la configuration réelle d'une pile AWS CloudFormation (AWS CloudFormation) diffère ou a dérivé de la configuration attendue. Une pile est considérée comme ayant dérivé si une ou plusieurs de ses ressources diffèrent de leur configuration attendue. La règle et la pile sont COMPLIANT lorsque le statut d'écart de la pile est IN_SYNC. La règle est NON_COMPLIANT si le statut d'écart de la pile est DRIFTED.

> **Note**
>
> Cette règle effectue l' DetectStackDrift opération sur chaque pile de votre compte. L' DetectStackDrift opération peut prendre plusieurs minutes, selon le nombre de ressources contenues dans la pile. Étant donné que la durée d'exécution maximale de cette règle est limitée à 15 minutes, il se peut que cette dernière expire avant que toutes les piles de votre compte aient été évaluées.
> Si vous rencontrez ce problème, nous vous recommandons de limiter le nombre de piles concernées par la règle à l'aide de balises. Vous pouvez effectuer les actions suivantes :
>
> 1. Divisez vos piles en groupes, chacun avec une balise différente.
> 2. Appliquez la même balise à toutes les piles de ce groupe.
> 3. Utilisez plusieurs instances de cette règle dans votre compte, chacune étant associée à une balise différente. Chaque instance de la règle peut ainsi traiter uniquement les piles dont la balise correspondante est mentionnée dans sa portée.

Identificateur : CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

Types de ressources : AWS::CloudFormation::Stack

Type de déclencheur : modifications de configuration et périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

formation de nuages RoleArn, Type : chaîne

> Le nom de ressource Amazon (ARN) du rôle IAM avec les autorisations politiques permettant de détecter la dérive des AWS CloudFormation piles. Pour plus d'informations sur les autorisations IAM requises pour le rôle, consultez la section Détection des modifications de configuration non gérées apportées aux piles et aux ressources | Considérations relatives à la détection d'une dérive dans le Guide de l' AWS CloudFormation utilisateur.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudformation-stack-notification-check

Vérifie si vos CloudFormation piles envoient des notifications d'événements à une rubrique Amazon SNS. (Facultatif) Vérifie si les rubriques Amazon SNS spécifiées sont utilisées. La règle est NON_COMPLIANT si les CloudFormation piles n'envoient pas de notifications.

Identificateur : CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Types de ressources : AWS::CloudFormation::Stack

Type de déclencheur : changements de configuration

Région AWS: Disponible uniquement en Chine (Pékin), Asie-Pacifique (Mumbai), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (Sao Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Asie-Pacifique (Centre), Chine (Ning) Région (Xia)

Paramètres :

snsTopic1 (facultatif), Type : chaîne

ARN de rubrique SNS.

snsTopic2 (facultatif), Type : chaîne

ARN de rubrique SNS.

snsTopic3 (facultatif), Type : chaîne

ARN de rubrique SNS.

snsTopic4 (facultatif), Type : chaîne

ARN de rubrique SNS.

snsTopic5 (facultatif), Type : chaîne

ARN de rubrique SNS.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

cloudfront-accesslogs-enabled

Vérifie si les CloudFront distributions Amazon sont configurées pour fournir des journaux d'accès à un compartiment Amazon S3. La règle est NON_COMPLIANT si la journalisation n'est pas configurée pour une CloudFront distribution.

Identificateur : CLOUDFRONT_ACCESSLOGS_ENABLED

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

S3 BucketName (facultatif), Type : chaîne

Nom du compartiment Amazon S3 pour stocker les journaux d'accès au serveur.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-associated-with-waf

Vérifie si les CloudFront distributions Amazon sont associées à un pare-feu d'application Web (WAF) ou à des listes de contrôle d'accès Web (ACL) WAFv2. La règle est NON_COMPLIANT si une CloudFront distribution n'est pas associée à une ACL Web WAF.

Identificateur : CLOUDFRONT_ASSOCIATED_WITH_WAF

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

waf WebAclIds (facultatif), Type : CSV

> Liste d'ID de listes ACL Web pour WAF ou d'Amazon Resource Names (ARN) de listes ACL Web pour WAFV2, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-custom-ssl-certificate

Vérifie si le certificat associé à une CloudFront distribution Amazon est le certificat SSL par défaut. La règle est NON_COMPLIANT si une CloudFront distribution utilise le certificat SSL par défaut.

Identificateur : CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-default-root-object-configured

Vérifie si une CloudFront distribution Amazon est configurée pour renvoyer un objet spécifique qui est l'objet racine par défaut. La règle est NON_COMPLIANT si aucun objet racine par défaut n'est configuré pour la CloudFront distribution Amazon.

Identificateur : CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-no-deprecated-ssl-protocols

Vérifie si les CloudFront distributions utilisent des protocoles SSL obsolètes pour la communication HTTPS entre les emplacements CloudFront périphériques et les origines personnalisées. Cette règle est NON_COMPLIED pour une CloudFront distribution si l'un des « OriginSsl protocoles » inclut « SSLv3 ».

Identificateur : CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-origin-access-identity-enabled

Vérifie si l'identité d'accès à l'origine est configurée pour la CloudFront distribution avec le type Amazon S3 Origin. La règle est NON_COMPLIANT si la CloudFront distribution est soutenue par S3 et qu'aucun type d'origine n'est configuré par OAI, ou si l'origine n'est pas un compartiment S3.

> **Note**
>
> La règle ne renvoie pas NOT_APPLICABLE si l'origine n'est pas un compartiment S3.

Identificateur : CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-origin-failover-enabled

Vérifie si un groupe d'origine est configuré pour la distribution d'au moins deux origines dans le groupe d'origine pour Amazon CloudFront. La règle est NON_COMPLIANT s'il n'existe aucun groupe d'origine pour la distribution.

Identificateur : CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

cloudfront-s3-origin-access-control-enabled

Vérifie si le contrôle d'accès à l'origine (OAC) est activé pour une CloudFront distribution Amazon avec un type d'origine Amazon Simple Storage Service (Amazon S3). La règle est NON_COMPLIANT pour les CloudFront distributions dont l'origine est Amazon S3 et pour lesquelles l'OAC n'est pas activé.

Identificateur : CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-s3-origin-non-existent-bucket

Vérifie si CloudFront les distributions Amazon pointent vers un compartiment S3 inexistant. La règle est NON_COMPLIANT si « S3 OriginConfig » pour une CloudFront distribution pointe vers un compartiment S3 inexistant. La règle n'évalue pas les compartiments S3 associé à un hébergement de site Web statique.

Identificateur : CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : périodique

Région AWS : uniquement disponible dans les régions Chine (Beijing) et USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-security-policy-check

Vérifie si les CloudFront distributions Amazon utilisent une politique de sécurité minimale et une suite de chiffrement TLSv1.2 ou supérieure pour les connexions des utilisateurs. Cette règle est NON CONFORME pour une CloudFront distribution si elle minimumProtocolVersion est inférieure à TLSv1.2_2018.

Identificateur : CLOUDFRONT_SECURITY_POLICY_CHECK

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-sni-enabled

Vérifie si les CloudFront distributions Amazon utilisent un certificat SSL personnalisé et sont configurées pour utiliser le SNI pour traiter les requêtes HTTPS. La règle est NON_COMPLIANT si un certificat SSL personnalisé est associé et si la méthode de prise en charge SSL est une adresse IP dédiée.

Identificateur : CLOUDFRONT_SNI_ENABLED

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-traffic-to-origin-encrypted

Vérifie si les CloudFront distributions Amazon chiffrent le trafic vers des origines personnalisées. La règle est NON_COMPLIANT si « OriginProtocol Policy » est « http uniquement » ou si « Policy » est « match-viewer » et « OriginProtocol Policy » est « allow-all ». ViewerProtocol

Identificateur : CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudfront-viewer-policy-https

Vérifie si vos CloudFront distributions Amazon utilisent le protocole HTTPS (directement ou via une redirection). La règle est NON_COMPLIANT si la valeur de ViewerProtocolPolicy est définie sur « allow-all » pour le ou pour le DefaultCacheBehavior . CacheBehaviors

Identificateur : CLOUDFRONT_VIEWER_POLICY_HTTPS

Types de ressources : AWS::CloudFront::Distribution

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

Cloudtrail-all-read-s3-data-event-check

Vérifie si un AWS CloudTrail suivi multirégional est activé et enregistre tous les événements de lecture de données S3 pour vos compartiments. La règle est NON_COMPLIANT si aucun journal multirégional ne consigne tous les types d'événements de données S3 lus pour tous les compartiments S3 actuels et futurs.

Identifiant : CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

vérification des événements de données cloudtrail-all-write-s3

Vérifie si un AWS CloudTrail suivi multirégional est activé et enregistre tous les événements d'écriture de données S3 pour vos compartiments. La règle est NON_COMPLIANT si aucun journal de suivi multirégional n'écrit tous les types d'événements de données S3 pour tous les compartiments S3 actuels et futurs.

Identifiant : CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail

Vérifie si la journalisation des accès au serveur Amazon S3 est activée dans les configurations du compartiment S3 pour vos AWS CloudTrail journaux. La règle est NON_COMPLIANT si la journalisation des accès au serveur S3 n'est pas CloudTrail activée dans au moins un compartiment S3 pour un trail.

Identifiant : CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

Types de ressources : AWS::CloudTrail::Trail

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

accès public à cloudtrail-s3-bucket interdit

Vérifie si les configurations du compartiment S3 pour vos AWS CloudTrail journaux bloquent l'accès public. La règle est NON_COMPLIANT si au moins un compartiment S3 pour un CloudTrail parcours est accessible au public.

Identifiant : CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBED

Types de ressources : AWS::CloudTrail::Trail

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudtrail-s3-dataevents-enabled

Vérifie si au moins une AWS CloudTrail piste enregistre les événements de données Amazon Simple Storage Service (Amazon S3) pour tous les compartiments S3. La règle est NON_COMPLIANT s'il existe des journaux de suivi ou si aucun journal de suivi n'enregistre des événements de données S3.

Identificateur : CLOUDTRAIL_S3_DATAEVENTS_ENABLED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

S3 BucketNames (facultatif), Type : chaîne

> Liste de noms de compartiment S3 séparés par des virgules pour lesquels la journalisation des événements de données doit être activée. Contrôles de comportement par défaut pour tous les compartiments S3.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudtrail-security-trail-enabled

Vérifie qu'il existe au moins une AWS CloudTrail piste définie conformément aux meilleures pratiques de sécurité. Cette règle est COMPLIANT si au moins un journal de suivi répond à toutes les conditions suivantes :

- enregistre les événements de services mondiaux
- est un journal de suivi multi-régions
- applique la validation des fichiers journaux

- chiffré avec une clé KMS
- enregistre les événements pour les lectures et les écritures
- enregistre les événements de gestion
- n'exclut aucun événement de gestion

Cette règle est NON_COMPLIANT si aucun journal de suivi ne répond à tous les critères mentionnés ci-dessus.

Identificateur : CLOUDTRAIL_SECURITY_TRAIL_ENABLED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudwatch-alarm-action-check

Vérifie si une action des CloudWatch alarmes est configurée pour l'état ALARM, INSUSUFFISENT_DATA ou OK. (Facultatif) Vérifie si des actions correspondent à un ARN nommé. La règle est NON_COMPLIANT si aucune action n'est spécifiée pour l'alarme ou le paramètre facultatif.

Identificateur : CLOUDWATCH_ALARM_ACTION_CHECK

Types de ressources : AWS::CloudWatch::Alarm

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

alarme ActionRequired, Type : chaîne, Valeur par défaut : true

Les alarmes ont au moins une action.

insuffisant DataAction Nécessaire, Type : chaîne, Valeur par défaut : true

Les alarmes ont au moins une action lorsque l'alarme active un état INSUFFICIENT_DATA à partir de n'importe quel autre état.

ok ActionRequired, Type : chaîne, Valeur par défaut : false

Les alarmes ont au moins une action lorsque l'alarme active un état OK à partir de n'importe quel autre état.

action1 (facultatif), Type : chaîne

L'action à exécuter, spécifiée sous forme d'ARN.

action2 (facultatif), Type : chaîne

L'action à exécuter, spécifiée sous forme d'ARN.

action3 (facultatif), Type : chaîne

L'action à exécuter, spécifiée sous forme d'ARN.

action4 (facultatif), Type : chaîne

L'action à exécuter, spécifiée sous forme d'ARN.

action5 (facultatif), Type : chaîne

L'action à exécuter, spécifiée sous forme d'ARN.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudwatch-alarm-action-enabled-check

Vérifie si les actions d' CloudWatch alarme Amazon sont activées. La règle est NON_COMPLIANT si les actions d' CloudWatch alarme ne sont pas activées.

Identificateur : CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

Types de ressources : AWS::CloudWatch::Alarm

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudwatch-alarm-resource-check

Vérifie si un type de ressource possède une CloudWatch alarme pour la métrique nommée. Vous pouvez spécifier des volumes EBS, des instances EC2, des clusters Amazon RDS ou des compartiments S3 pour le type de ressource. La règle est CONFORME si la métrique nommée possède un identifiant de ressource et une CloudWatch alarme.

Identificateur : CLOUDWATCH_ALARM_RESOURCE_CHECK

Types de ressources : AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceType, Type : chaîne

AWS type de ressource. La valeur peut être l'une des suivantes : AWS::EC2::Volume, AWS::EC2::Instance, AWS::RDS::DBCluster, or AWS::S3::Bucket.

metricName, Type : chaîne

Le nom de la métrique associée à l'alarme (par exemple, « CPUUtilization » pour les instances EC2).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudwatch-alarm-settings-check

Vérifie si les CloudWatch alarmes portant le nom de métrique donné possèdent les paramètres spécifiés.

Identificateur : CLOUDWATCH_ALARM_SETTINGS_CHECK

Types de ressources : AWS::CloudWatch::Alarm

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

metricName, Type : chaîne

Nom de la métrique associée à l'alarme.

threshold (facultatif), Type : int

Valeur à laquelle la statistique spécifiée est comparée.

evaluationPeriods (facultatif), Type : int

Nombre de périodes au cours desquelles les données sont comparées au seuil défini.

period (facultatif), Type : int, Valeur par défaut : 300

La période, en secondes, au cours de laquelle la statistique spécifiée est appliquée.

comparisonOperator (facultatif), Type : chaîne

Opération de comparaison de la statistique et du seuil spécifiés (par exemple, « GreaterThan Seuil »).

statistic (facultatif), Type : chaîne

La statistique de la métrique associée à l'alarme (par exemple, « Average » ou « Sum »).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudwatch-log-group-encrypted

Vérifie si les groupes Amazon CloudWatch Log sont chiffrés à l'aide d'une clé AWS KMS ou d'un identifiant de clé AWS KMS spécifié. La règle est NON_COMPLIED si un groupe de CloudWatch journaux n'est pas chiffré avec une clé KMS ou est chiffré avec une clé KMS non fournie dans le paramètre de règle.

Identificateur : CLOUDWATCH_LOG_GROUP_ENCRYPTED

Types de ressources : AWS::Logs::LogGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

KmsKeyId (Facultatif), Type : chaîne

Amazon Resource Name (ARN) de l'ID de la clé KMS utilisée pour chiffrer le groupe de journaux.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloud-trail-cloud-watch-logs-enabled

Vérifie si les AWS CloudTrail sentiers sont configurés pour envoyer des journaux aux CloudWatch journaux. Le sentier est NON_COMPLIANT si CloudWatchLogsLogGroupArn sa propriété est vide.

Identificateur : CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

Types de ressources : AWS::CloudTrail::Trail

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

attendu DeliveryWindowAge (facultatif), Type : int

Âge maximum, en heures, lors de la dernière livraison CloudWatch des journaux conformes aux normes.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloudtrail-enabled

> **Important**
>
> L'identificateur (CLOUD_TRAIL_ENABLED) et le nom (cloudtrail-enabled) de cette règle sont différents.

Vérifie si AWS CloudTrail un suivi est activé dans votre AWS compte. La règle est NON_COMPLIANT si aucun journal de suivi n'est activé. Facultativement, la règle vérifie un compartiment S3, une rubrique Amazon Simple Notification Service (Amazon SNS) et un groupe de journaux spécifiques. CloudWatch

Identificateur : CLOUD_TRAIL_ENABLED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

s3 BucketName (facultatif), Type : chaîne

Nom du compartiment S3 CloudTrail auquel les fichiers journaux doivent être envoyés.

snsTopicArn (Facultatif), Type : chaîne

ARN de la rubrique SNS CloudTrail à utiliser pour les notifications.

cloud WatchLogsLogGroupArn (facultatif), Type : chaîne

CloudWatch ARN du groupe de logs CloudTrail auquel envoyer les données.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloud-trail-encryption-enabled

Vérifie s' AWS CloudTrail il est configuré pour utiliser le chiffrement côté serveur (SSE AWS KMS) AWS Key Management Service (). La règle est CONFORME si elle KmsKeyId est définie.

Identificateur : CLOUD_TRAIL_ENCRYPTION_ENABLED

Types de ressources : AWS::CloudTrail::Trail

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cloud-trail-log-file-validation-enabled

Vérifie s'il AWS CloudTrail crée un fichier de résumé signé avec des journaux. AWS recommande que la validation des fichiers soit activée sur tous les sentiers. La règle est NON_COMPLIANT si la validation n'est pas activée.

Identificateur : CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

Types de ressources : AWS::CloudTrail::Trail

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

cmk-backing-key-rotation-enabled

Vérifie si la rotation automatique des clés est activée pour chaque clé et correspond à l'ID de clé AWS KMS créée par le client. La règle est NON_COMPLIANT si le rôle d'enregistreur AWS Config pour une ressource ne dispose pas de l'autorisation kms :DescribeKey .

> **Note**
>
> La rotation automatique des clés n'est pas prise en charge pour les clés KMS asymétriques, les clés KMS HMAC, les clés KMS présentant des éléments de clé importés ou les clés KMS dans des magasins de clés personnalisés.

Identificateur : CMK_BACKING_KEY_ROTATION_ENABLED

Types de ressources : AWS::KMS::Key

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

codebuild-project-artifact-encryption

Vérifie si le chiffrement est activé pour tous les artefacts d'un AWS CodeBuild projet. La règle est NON_COMPLIANT si « EncryptionDisabled » est défini sur « true » pour toute configuration d'artefact principale ou secondaire (le cas échéant).

Identificateur : CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

Types de ressources : AWS::CodeBuild::Project

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

codebuild-project-environment-privileged-check

Vérifie si le mode privilégié est activé dans un environnement de AWS CodeBuild projet. La règle est NON_COMPLIANT pour un CodeBuild projet si « PrivilegedMode » est défini sur « true ».

Identificateur : CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

Types de ressources : AWS::CodeBuild::Project

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

exemptedProjects (facultatif), Type : CSV

> Liste séparée par des virgules des noms de CodeBuild projets autorisés à avoir « PrivilegedMode » avec la valeur « true ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

codebuild-project-envvar-awscred-check

Vérifie si le projet contient les variables d'environnement _ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY. AWS La règle est NON_COMPLIANT lorsque les variables d'environnement du projet contiennent des informations d'identification en texte brut.

Identifiant : CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK

Types de ressources : AWS::CodeBuild::Project

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

codebuild-project-logging-enabled

Vérifie si au moins une option de journalisation est activée dans un environnement de AWS CodeBuild projet. La règle est NON_COMPLIANT si le statut de toutes les configurations de journal actuelles est défini sur « DISABLED ».

Identificateur : CODEBUILD_PROJECT_LOGGING_ENABLED

Types de ressources : AWS::CodeBuild::Project

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

s3 BucketNames (facultatif), Type : chaîne

Liste de noms de compartiments Amazon S3 séparés par des virgules auxquels les journaux doivent être envoyés si les journaux S3 sont configurés.

cloud WatchGroupNames (facultatif), Type : chaîne

Liste séparée par des virgules des noms des groupes de CloudWatch journaux Amazon auxquels les journaux doivent être envoyés si les CloudWatch journaux sont configurés.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

codebuild-project-s3-logs-encrypted

Vérifie si le chiffrement des journaux d'un AWS CodeBuild projet configuré avec Amazon S3 Logs est activé. La règle est NON_COMPLIANT si « EncryptionDisabled » est défini sur « true » dans la S3 LogsConfig d'un projet. CodeBuild

Identificateur : CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

Types de ressources : AWS::CodeBuild::Project

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

exemptedProjects (facultatif), Type : CSV

Liste séparée par des virgules des noms de CodeBuild projets autorisés à générer des journaux non chiffrés.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

codebuild-project-source-repo-url-check

Vérifie si l'URL du référentiel source Bitbucket contient des informations d'identification de connexion ou non. La règle est NON_COMPLIANT si l'URL contient des informations d'identification de connexion et COMPLIANT si ce n'est pas le cas.

Identificateur : CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Types de ressources : AWS::CodeBuild::Project

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

codedeploy-auto-rollback-monitor-enabled

Vérifie si la restauration et la surveillance automatiques du déploiement avec les alarmes associées sont activées pour le groupe de déploiement. La règle est NON_COMPLIANT si elle n' AlarmConfiguration a pas été configurée AutoRollbackConfiguration ou si elle n'est pas activée.

Identificateur : CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

Types de ressources : AWS::CodeDeploy::DeploymentGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

codedeploy-ec2-minimum-healthy-hosts-configured

Vérifie si le groupe de déploiement pour la plateforme de calcul EC2/sur site est configuré avec un pourcentage minimum de flotte d'hôtes sains ou un nombre d'hôtes supérieur ou égal au seuil d'entrée. La règle est NON_COMPLIANT si l'une de ces deux valeurs est inférieure au seuil.

Identificateur : CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

Types de ressources : AWS::CodeDeploy::DeploymentGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

minimum HealthyHostsFleetPercent (facultatif), Type : int, Valeur par défaut : 66

Pourcentage minimal de flotte d'hôtes sains au cours du déploiement. La valeur par défaut est de 66 %.

minimum HealthyHostsHostCount (facultatif), Type : int, Valeur par défaut : 1

Pourcentage minimal d'hôtes sains dans la flotte au cours du déploiement. La valeur par défaut est de 1.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

codedeploy-lambda-allatonce-traffic-shift-disabled

Vérifie si le groupe de déploiement de la plateforme de calcul Lambda n'utilise pas la configuration de déploiement par défaut. La règle est NON_COMPLIANT si le groupe de déploiement utilise la configuration de déploiement « Par défaut ». CodeDeploy LambdaAllAtOnce'.

Identificateur : CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

Types de ressources : AWS::CodeDeploy::DeploymentGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

codepipeline-deployment-count-check

Vérifie si la première étape de déploiement de AWS CodePipeline effectue plusieurs déploiements. (Facultatif) Vérifie si chacune des étapes restantes effectue plus de déploiements que le nombre spécifié (`deploymentLimit`).

Identificateur : CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Types de ressources : AWS::CodePipeline::Pipeline

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney) et Canada (Centre)

Paramètres :

deploymentLimit (facultatif), Type : int

Nombre maximal de déploiements que chaque étape peut exécuter.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

codepipeline-region-fanout-check

Vérifie si chaque étape des AWS CodePipeline déploiements représente plus de N fois le nombre de régions déployées lors de toutes les étapes combinées précédentes, où N est le numéro de fanout de la région. AWS CodePipeline La première étape de déploiement peut déployer une région au maximum et la deuxième étape de déploiement peut déployer un nombre maximum spécifié dans `regionFanoutFactor`. Si vous ne fournissez pas de `regionFanoutFactor`, la valeur par défaut est trois. Par exemple : si la première étape de déploiement déploie sur une région et que la 2e étape de déploiement déploie sur trois régions, la 3e étape de déploiement peut déployer sur 12 régions, c'est-à-dire, la somme des étapes précédentes multipliée par le numéro de diffusion en éventail de la région (trois). La règle est NON_COMPLIANT si le déploiement est dans plus d'une région dans la première étape ou dans trois régions dans la 2e étape ou 12 régions dans la 3e étape.

Identificateur : CODEPIPELINE_REGION_FANOUT_CHECK

Types de ressources : AWS::CodePipeline::Pipeline

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney) et Canada (Centre)

Paramètres :

regionFanoutFactor (Facultatif), Type : int, Valeur par défaut : 3

> Le nombre de régions dans lesquelles AWS CodePipeline il a été déployé lors de toutes les étapes précédentes est le nombre acceptable de régions dans lesquelles chaque étape peut être déployée.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

custom-eventbus-policy-attached

Vérifie si les bus d'événements EventBridge personnalisés Amazon sont associés à une politique basée sur les ressources. La règle est NON_COMPLIANT si une politique de bus d'événements personnalisés n'est associée à aucune politique basée sur les ressources.

Identificateur : CUSTOM_EVENTBUS_POLICY_ATTACHED

Types de ressources : AWS::Events::EventBus

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

custom-schema-registry-policy-attached

Vérifie si les registres de EventBridge schémas Amazon personnalisés sont associés à une politique de ressources. La règle est NON_COMPLIANT pour les registres de schémas personnalisés qui ne sont associés à aucune politique de ressource.

Identificateur : CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

Types de ressources : AWS::EventSchemas::Registry

Type de déclencheur : périodique

Région AWS: Disponible uniquement en Europe (Stockholm), Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (Sao Paulo), Asie-Pacifique (Hong Kong), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), région du Canada (centre)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

cw-loggroup-retention-period-check

Vérifie si une période de CloudWatch LogGroup rétention Amazon est définie sur plus de 365 jours ou si elle est définie sur une période de rétention spécifiée. La règle est NON_COMPLIANT si la période de rétention est inférieure`MinRetentionTime`, si elle est spécifiée, ou à 365 jours.

> **Note**
>
> Si le paramètre de conservation est défini sur « Never expire » pour un groupe de journaux, la règle est marquée comme COMPLIANT.

Identificateur : CW_LOGGROUP_RETENTION_PERIOD_CHECK

Types de ressources : AWS::Logs::LogGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

LogGroupNames (Facultatif), Type : CSV

Une liste de noms de groupe de journaux permettant de vérifier la période de conservation, séparés par des virgules.

MinRetentionTime (Facultatif), Type : int

Indiquez la durée de conservation. Les valeurs possibles sont : 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 et 3653. La période de conservation par défaut est de 365 jours.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dax-encryption-enabled

Vérifie si les clusters Amazon DynamoDB Accelerator (DAX) sont chiffrés. La règle est NON_COMPLIANT si un cluster DAX n'est pas chiffré.

Identificateur : DAX_ENCRYPTION_ENABLED

Types de ressources : AWS::DAX::Cluster

Type de déclencheur : périodique

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

chiffrement des points de terminaison dax-tls

Vérifie si votre cluster ClusterEndpointEncryptionType Amazon DynamoDB Accelerator (DAX) est configuré sur TLS. La règle est NON_COMPLIANT si un cluster DAX n'est pas chiffré par le protocole TLS (Transport Layer Security).

Identifiant : DAX_TLS_ENDPOINT_ENCRYPTION

Types de ressources : AWS::DAX::Cluster

Type de déclencheur : périodique

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

db-instance-backup-enabled

Vérifie si les sauvegardes sont activées pour les instances de bases de données RDS. Le cas échéant, la règle vérifie la période de conservation des sauvegardes et la fenêtre de sauvegarde.

Identificateur : DB_INSTANCE_BACKUP_ENABLED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

backupRetentionPeriod (Facultatif), Type : int

Période de conservation des sauvegardes.

backupRetentionMinimum (Facultatif), Type : int

Période de conservation minimale des sauvegardes.

preferredBackupWindow (Facultatif), Type : chaîne

Plage de temps au cours de laquelle les sauvegardes sont créées.

checkReadReplicas (Facultatif), Type : valeur booléenne

Vérifie si les sauvegardes sont activées pour les réplicas en lecture des instances de bases de données RDS.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

desired-instance-tenancy

Vérifie la valeur « tenancy » des instances EC2. Vérifie également si les ID d'AMI sont spécifiés pour être lancés à partir de ces AMI ou si les ID d'hôte sont lancés sur ces hôtes dédiés. La règle est CONFORME si l'instance correspond à un hôte et à une AMI, si elle est spécifiée, dans une liste.

Identificateur : DESIRED_INSTANCE_TENANCY

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

location, Type : chaîne

Location souhaitée des instances. Les valeurs valides sont DEDICATED, HOST et DEFAULT.

imageId (facultatif), Type : CSV

La règle évalue les instances lancées uniquement à partir d'AMI présentant les ID spécifiés. S'il y a plusieurs ID d'AMI, séparez-les à l'aide de virgules.

hostId (facultatif), Type : CSV

Les ID des hôtes dédiés EC2 sur lesquels les instances doivent être lancées. S'il y a plusieurs ID d'hôte, séparez-les à l'aide de virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

desired-instance-type

Vérifie si les instances EC2 présentent un type d'instance spécifique. La règle est NON_COMPLIANT si aucune instance EC2 n'est spécifiée dans la liste des paramètres. Pour obtenir la liste des types

d'instances EC2 pris en charge, veuillez consulter la section Types d'instances dans le Guide de l'utilisateur EC2 pour les instances Linux.

Identificateur : DESIRED_INSTANCE_TYPE

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

instanceType, Type : CSV

Liste de types d'instances EC2 (par exemple, « t2.small, m4.large, i2.xlarge »), séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir Création de règles gérées AWS Config avec des modèles AWS CloudFormation.

dms-auto-minor-version-upgrade-check

Vérifie si les mises à niveau automatiques des versions mineures sont activées sur une instance de réplication du Service de migration de AWS base de données (AWS DMS). La règle est NON_COMPLIANT si une instance de réplication AWS DMS n'est pas configurée avec des mises à niveau automatiques de versions mineures.

Identificateur : DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

Types de ressources : AWS::DMS::ReplicationInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dms-endpoint-ssl-configured

Vérifie si les points de terminaison du AWS Database Migration Service (AWS DMS) sont configurés avec une connexion SSL. La règle est NON_COMPLIANT si aucune connexion SSL n'est configurée pour AWS DMS.

Identificateur : DMS_ENDPOINT_SSL_CONFIGURED

Types de ressources : AWS::DMS::Endpoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

Authentification DMS-MONGO-DB activée

Vérifie si les points de terminaison du AWS Database Migration Service (AWS DMS) pour les magasins de MongoDb données sont activés pour l'authentification par mot de passe et le contrôle d'accès. La règle est NON_COMPLIANT si l'authentification par mot de passe et le contrôle d'accès ne sont pas activés.

Identifiant : DMS_MONGO_DB_AUTHENTICATION_ENABLED

Types de ressources : AWS::DMS::Endpoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

Autorisation DMS-NEPTUNE-IAM activée

Vérifie si un point de terminaison du AWS Database Migration Service (AWS DMS) pour les bases de données Amazon Neptune est configuré avec l'autorisation IAM. La règle est NON_COMPLIANT si un point de AWS terminaison DMS dont Neptune est la cible est défini sur false. IamAuthEnabled

Identifiant : DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

Types de ressources : AWS::DMS::Endpoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

compatible DMS-REDIS-TLS

Vérifie si les points de terminaison du AWS Database Migration Service (AWS DMS) pour les magasins de données Redis sont activés pour le chiffrement TLS/SSL des données communiquées avec d'autres points de terminaison. La règle est NON_COMPLIANT si le chiffrement TLS/SSL n'est pas activé.

Identifiant : DMS_REDIS_TLS_ENABLED

Types de ressources : AWS::DMS::Endpoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dms-replication-not-public

Vérifie si les instances de réplication du AWS Database Migration Service (AWS DMS) sont publiques. La règle est NON_COMPLIANT si PubliclyAccessible le champ est défini sur true.

Identificateur : DMS_REPLICATION_NOT_PUBLIC

Types de ressources : AWS::DMS::ReplicationInstance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dms-replication-task-sourcedb-logging

Vérifie si la journalisation est activée avec un niveau de gravité valide pour les tâches de réplication AWS DMS d'une base de données source. La règle est NON_COMPLIANT si la journalisation n'est pas activée ou si les journaux des tâches de réplication DMS d'une base de données source présentent un niveau de gravité non valide.

Identificateur : DMS_REPLICATION_TASK_SOURCEDB_LOGGING

Types de ressources : AWS::DMS::ReplicationTask

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dms-replication-task-targetdb-logging

Vérifie si la journalisation est activée avec un niveau de gravité valide pour les événements des tâches de réplication AWS DMS d'une base de données cible. La règle est NON_COMPLIANT si la journalisation n'est pas activée ou si la journalisation des tâches de réplication d'une base de données cible présente un niveau de gravité non valide.

Identificateur : DMS_REPLICATION_TASK_TARGETDB_LOGGING

Types de ressources : AWS::DMS::ReplicationTask

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

docdb-cluster-audit-logging-enabled

Vérifie si l'exportation des journaux est activée pour un cluster d'instances Amazon DocumentDB (compatible avec MongoDB) pour les CloudWatch journaux d'audit. La règle est NON_COMPLIANT

si l'exportation des journaux n'est pas CloudWatch activée pour les journaux d'audit d'un cluster d'instances Amazon DocumentDB.

Identificateur : DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Europe (Milan), Asie-Pacifique (Tokyo), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Canada (Centre) et Chine (Ningxia)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

docdb-cluster-backup-retention-check

Vérifie si la période de conservation d'un cluster de bases de données Amazon Document est définie sur un nombre de jours spécifique. La règle est NON_COMPLIANT si la période de conservation est inférieure à la valeur spécifiée par le paramètre.

Identificateur : DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Europe (Milan), Asie-Pacifique (Tokyo), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Canada (Centre) et Chine (Ningxia)

Paramètres :

minimum BackupRetentionPeriod (facultatif), Type : int

Les sauvegardes doivent être conservées pendant un nombre minimal de jours. Les valeurs valides sont comprises entre 1 et 35, la valeur par défaut est 7. Cette règle est NON_COMPLIANT si la valeur est supérieure à « sauvegarde »RetentionPeriod.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

docdb-cluster-deletion-protection-enabled

Vérifie si la protection contre la suppression est activée sur un cluster Amazon DocumentDB (compatible avec MongoDB). La règle est NON_COMPLIANT si le champ deletionProtection d'un cluster Amazon DocumentDB est défini sur false.

Identificateur : DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Europe (Milan), Asie-Pacifique (Tokyo), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Canada (Centre) et Chine (Ningxia)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

docdb-cluster-encrypted

Vérifie si le chiffrement du stockage est activé pour les clusters Amazon DocumentDB (compatible avec MongoDB). La règle est NON_COMPLIANT si le chiffrement du stockage n'est pas activé.

Identificateur : DOCDB_CLUSTER_ENCRYPTED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Europe (Milan), Asie-Pacifique (Tokyo), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Canada (Centre) et Chine (Ningxia)

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

> Liste séparée par des virgules des ARN des clés KMS à comparer avec l' KmsKeyID du cluster chiffré.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

docdb-cluster-snapshot-public-prohibited

Vérifie si les instantanés de clusters manuels Amazon DocumentDB sont publics. La règle est NON_COMPLIANT si des instantanés de clusters manuels Amazon DocumentDB sont publics.

Identificateur : DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Types de ressources : AWS : :RDS : :DB ClusterSnapshot

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Europe (Milan), Asie-Pacifique (Tokyo), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney) et Canada (Centre)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-autoscaling-enabled

Vérifie si les tables Amazon DynamoDB ou les index secondaires globaux peuvent traiter la capacité en lecture/écriture en mode à la demande ou en mode provisionné si l'autoscaling automatique est activé. La règle est NON_COMPLIANT si l'un des modes est utilisé sans que l'autoscaling ne soit activé

Identificateur : DYNAMODB_AUTOSCALING_ENABLED

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

min ProvisionedReadCapacity (facultatif), Type : int

Nombre minimum d'unités qui doivent être mises en service avec une capacité en lecture dans le groupe Auto Scaling.

max ProvisionedReadCapacity (facultatif), Type : int

Nombre maximum d'unités qui doivent être mises en service avec une capacité en lecture dans le groupe Auto Scaling.

targetReadUtilization (Facultatif), Type : double

Pourcentage d'utilisation cible de la capacité en lecture. L'utilisation cible est exprimée en termes de ratio de capacité consommée par rapport à la capacité allouée.

min ProvisionedWriteCapacity (facultatif), Type : int

Nombre minimum d'unités qui doivent être mises en service avec une capacité en écriture dans le groupe Auto Scaling.

max ProvisionedWriteCapacity (facultatif), Type : int

Nombre maximum d'unités qui doivent être mises en service avec une capacité en écriture dans le groupe Auto Scaling.

targetWriteUtilization (Facultatif), Type : double

Pourcentage d'utilisation cible de la capacité en écriture. L'utilisation cible est exprimée en termes de ratio de capacité consommée par rapport à la capacité allouée.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-in-backup-plan

Vérifie si la table Amazon DynamoDB est présente dans AWS Backup Plans. La règle est NON_COMPLIANT si les tables Amazon DynamoDB ne sont présentes dans aucun plan Backup. AWS

Identificateur : DYNAMODB_IN_BACKUP_PLAN

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour les tables Amazon DynamoDB au cours de la période spécifiée. La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans la table DynamoDB.

Identificateur : DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des tables DynamoDB pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

Nom de la table DynamoDB pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

dynamodb-meets-restore-time-target

Vérifie si la durée de restauration des tables Amazon DynamoDB correspond à la durée spécifiée. La règle est NON_COMPLIANT si LatestRestoreExecutionTimeMinutes une table DynamoDB est supérieure à quelques minutes. maxRestoreTime

Identifiant : DYNAMODB_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balises des tables DynamoDB pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

Nom de la table DynamoDB pour la règle à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-pitr-enabled

Vérifie si point-in-time la restauration (PITR) est activée pour les tables Amazon DynamoDB. La règle est NON_COMPLIANT si la PITR n'est pas activée.

Identificateur : DYNAMODB_PITR_ENABLED

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-resources-protected-by-backup-plan

Vérifie si les tables Amazon DynamoDB sont protégées par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué à la table DynamoDB.

Identificateur : DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des tables DynamoDB pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

Nom de la table DynamoDB pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-table-deletion-protection-enabled

Vérifie si la protection contre la suppression d'une table Amazon DynamoDB a été activée. La règle est NON_COMPLIANT si la protection contre la suppression de la table est désactivée.

Identificateur : DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-table-encrypted-kms

Vérifie si la table Amazon DynamoDB est chiffrée AWS avec le service de gestion des clés (KMS). La règle est NON_COMPLIANT si la table Amazon DynamoDB n'est pas chiffrée avec KMS. AWS La règle est également NON_COMPLIANT si la clé AWS KMS chiffrée n'est pas présente dans le paramètre `kmsKeyArns` d'entrée.

Identificateur : DYNAMODB_TABLE_ENCRYPTED_KMS

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

Liste séparée par des virgules des ARN des clés AWS KMS autorisés pour le chiffrement des tables Amazon DynamoDB.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-table-encryption-enabled

Vérifie si les tables Amazon DynamoDB sont chiffrées et contrôle leur statut. La règle est COMPLIANT si le statut est activé ou en cours d'activation.

Identificateur : DYNAMODB_TABLE_ENCRYPTION_ENABLED

Types de ressources : AWS::DynamoDB::Table

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

dynamodb-throughput-limit-check

Vérifie si le débit DynamoDB provisionné s'approche de la limite maximale pour votre compte. Par défaut, la règle vérifie si le débit provisionné dépasse le seuil de 80 % des limites de votre compte.

Identificateur : DYNAMODB_THROUGHPUT_LIMIT_CHECK

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

AccountRCU ThresholdPercentage (facultatif), Type : int, Par défaut: 80

Pourcentage d'unités de capacité en lecture provisionnées pour votre compte. Lorsque cette valeur est atteinte, la règle est marquée noncompliant.

AccountWCU ThresholdPercentage (facultatif), Type : int, Par défaut: 80

Pourcentage d'unités de capacité en écriture provisionnées pour votre compte. Lorsque cette valeur est atteinte, la règle est marquée noncompliant.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ebs-in-backup-plan

Vérifiez si des volumes Amazon Elastic Block Store (Amazon EBS) sont ajoutés dans les plans de sauvegarde de Backup. AWS La règle est NON_COMPLIANT si aucun volume Amazon EBS n'est inclus dans les plans de sauvegarde.

Identificateur : EBS_IN_BACKUP_PLAN

Types de ressources : AWS::EC2::Volume

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ebs-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour Amazon Elastic Block Store (Amazon EBS). La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans le volume Amazon EBS.

Identificateur : EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::EC2::Volume

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balise des volumes Amazon EBS pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du volume Amazon EBS pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir Création de règles gérées AWS Config avec des modèles AWS CloudFormation.

ebs-meets-restore-time-target

Vérifie si la durée de restauration des volumes Amazon Elastic Block Store (Amazon EBS) est conforme à la durée spécifiée. La règle est NON_COMPLIANT si un

LatestRestoreExecutionTimeMinutes volume Amazon EBS est supérieur à quelques minutes. maxRestoreTime

Identifiant : EBS_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::EC2::Volume

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balise des volumes Amazon EBS pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

ID du volume Amazon EBS pour la règle à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ebs-optimized-instance

Vérifie si l'optimisation Amazon EBS est activée pour les instances Amazon Elastic Compute Cloud (Amazon EC2) susceptibles d'être optimisées pour Amazon EBS. La règle est NON_COMPLIANT si l'optimisation EBS n'est pas activée pour une instance Amazon EC2 susceptible d'être optimisée pour EBS.

> **Note**
>
> Les instances EC2 optimisées pour EBS par défaut renvoient en permanence `COMPLIANT` suite aux évaluations de règles.

Identificateur : EBS_OPTIMIZED_INSTANCE

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ebs-resources-protected-by-backup-plan

Vérifie si des volumes Amazon Elastic Block Store (Amazon EBS) sont protégés par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué au volume Amazon EBS.

Identificateur : EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::EC2::Volume

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balise des volumes Amazon EBS pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du volume Amazon EBS pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ebs-snapshot-public-restorable-check

Vérifie si les instantanés Amazon Elastic Block Store (Amazon EBS) ne sont pas publiquement restaurables. La règle est NON_COMPLIANT si un ou plusieurs instantanés avec RestorableByUserIds champ sont définis sur tous, c'est-à-dire que les instantanés Amazon EBS sont publics.

Identificateur : EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-client-vpn-connection-log-enabled

Vérifie si la journalisation des connexions AWS client est activée sur le point de terminaison du VPN client. La règle est NON_COMPLIANT s'il s'agit de « Configuration ». ConnectionLogOptions.Enabled' est défini sur « false ».

Identificateur : EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

Types de ressources : AWS::EC2::ClientVpn Endpoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-client-vpn-not-authorize-all

Vérifie si les règles d'autorisation du AWS Client VPN autorisent l'accès à la connexion pour tous les clients. La règle est NON_COMPLIANT si « AccessAll » est présent et défini sur true.

Identificateur : EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

Types de ressources : AWS::EC2::ClientVpn Endpoint

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-ebs-encryption-by-default

Vérifie si le chiffrement Amazon Elastic Block Store (EBS) est activé par défaut. La règle est NON_COMPLIANT si la validation n'est pas activée.

Identificateur : EC2_EBS_ENCRYPTION_BY_DEFAULT

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-imdsv2-check

Vérifie si la version des métadonnées de l'instance Amazon Elastic Compute Cloud (Amazon EC2) est configurée avec Instance Metadata Service Version 2 (IMDSv2). La règle est NON_COMPLIANT si elle HttpTokens est définie sur facultatif.

Identificateur : EC2_IMDSV2_CHECK

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ec2-instance-detailed-monitoring-enabled

Vérifie si la surveillance détaillée est activée pour les instances EC2. La règle est NON_COMPLIANT si la surveillance détaillée n'est pas activée.

Identificateur : EC2_INSTANCE_DETAILED_MONITORING_ENABLED

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ec2-instance-managed-by-systems-manager

> **Important**
>
> L'identificateur de cette règle (EC2_INSTANCE_MANAGED_BY_SSM) et son nom (ec2-instance-managed-by-systems-manager) sont différents.

Vérifie si vos instances Amazon EC2 sont gérées par AWS Systems Manager un agent (agent SSM). La règle est NON_COMPLIED si une instance EC2 est en cours d'exécution et que l'agent SSM est arrêté, ou si une instance EC2 est en cours d'exécution et que l'agent SSM est arrêté.

> **Note**
>
> La règle ne renverra pas NON_COMPLIANT si une instance EC2 est arrêtée et que l'agent SSM est en cours d'exécution.

Identificateur : EC2_INSTANCE_MANAGED_BY_SSM

Types de ressources : AWS::EC2::Instance, AWS::SSM::ManagedInstance Inventaire

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-instance-multiple-eni-check

Vérifie si Amazon Elastic Compute Cloud (Amazon EC2) utilise plusieurs interfaces réseau Elastic (ENI) ou Elastic Fabric Adapters (EFA). La règle est NON_COMPLIANT si une instance Amazon EC2 utilise plusieurs interfaces réseau.

Identificateur : EC2_INSTANCE_MULTIPLE_ENI_CHECK

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

NetworkInterfaceIds (Facultatif), Type : CSV

Liste d'ID d'instances réseau séparés par des virgules

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-instance-no-public-ip

Vérifie si les instances EC2 présentent une association d'adresse IP publique. La règle est NON_COMPLIANT si le champ publicIp est présent dans l'élément de configuration de l'instance EC2. Cette règle s'applique uniquement à IPv4.

Contexte : grâce aux adresses IP publiques, les instances EC2 sont directement accessibles sur Internet. Cette situation risque néanmoins de compromettre la sécurité ou la conformité :

- Sécurité : dans de nombreux cas, il n'est pas recommandé d'associer vos instances EC2 à des adresses IP publiques, sauf si elles doivent être accessibles au public. Si elle est associée à une adresse IP publique, votre instance EC2 est exposée à des risques de sécurité potentiels, tels qu'un accès non autorisé ou des attaques.

- Conformité : diverses normes de conformité telles que PCI, DSS ou HIPAA appliquent des exigences spécifiques concernant la segmentation du réseau et les contrôles d'accès. Ces exigences peuvent être satisfaites si les instances EC2 ne sont pas associées inutilement à des adresses IP publiques.
- Gestion des coûts : les adresses IP publiques peuvent engendrer des coûts supplémentaires, en particulier si elles sont associées à des instances EC2 en permanence. C'est en identifiant les instances EC2 présentant des adresses IP publiques inutiles que vous pourrez potentiellement réduire les coûts.

Identificateur : EC2_INSTANCE_NO_PUBLIC_IP

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-instance-profile-attached

Vérifie si un profil AWS Identity and Access Management (IAM) est associé à une instance EC2. La règle est NON_COMPLIANT si aucun profil IAM n'est associé à l'instance EC2.

Identificateur : EC2_INSTANCE_PROFILE_ATTACHED

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

IamInstanceProfileArnList (Facultatif), Type : CSV

Liste de profils IAM Amazon Resource Names (ARN) susceptibles d'être associés aux instances Amazon EC2, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour les instances Amazon Elastic Compute Cloud (Amazon EC2). La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans l'instance Amazon EC2.

Identificateur : EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::EC2::Instance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balise des instances Amazon EC2 pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID de l'instance Amazon EC2 pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-launch-template-public-ip-disabled

Vérifie si les modèles de lancement Amazon EC2 sont configurés pour attribuer des adresses IP publiques aux interfaces réseau. La règle est NON_COMPLIANT si la version par défaut d'un modèle de lancement EC2 possède au moins une interface réseau avec « » défini sur « vrai AssociatePublic IpAddress ».

Identificateur : EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

Types de ressources : AWS::EC2::LaunchTemplate

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

exemptedLaunchTemplates (Facultatif), Type : CSV

> Liste séparée par des virgules des identifiants de modèles de lancement EC2 exemptés autorisés à avoir des interfaces réseau dont la AssociatePublicIpAddress valeur est définie sur « vrai ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-managedinstance-applications-blacklisted

Vérifie qu'aucune des applications spécifiées n'est installée sur l'instance. Vous pouvez éventuellement indiquer la version. Les versions plus récentes ne seront pas placées sur liste noire. Si vous le souhaitez, précisez la plate-forme, pour n'appliquer la règle qu'aux instances qui exécutent cette plate-forme.

Identificateur : EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Types de ressources : AWS::SSM::ManagedInstance Inventaire

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

applicationNames, Type : CSV

Liste de noms d'applications séparés par des virgules. Si vous le souhaitez, spécifiez les versions ajoutées avec « : » (par exemple, « Chrome : 0.5.3, FireFox »).

> **Note**
>
> Les noms d'applications doivent être des correspondances exactes. Par exemple, utilisez **`firefox`** sous Linux ou **`firefox-compat`** sous Amazon Linux. En outre, AWS Config ne prend actuellement pas en charge les caractères génériques pour le paramètre ApplicationNames (par exemple,). **`firefox*`**

platformType (facultatif), Type : chaîne

Type de plateforme (par exemple, « Linux » ou « Windows »).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

ec2-managedinstance-applications-required

Vérifie qu'aucune des applications spécifiées n'est installée sur l'instance. Si vous le souhaitez, spécifiez la version minimum acceptable. Vous pouvez également préciser la plate-forme afin que la règle ne s'applique qu'aux instances qui exécutent cette plate-forme.

> **Note**
>
> Vérifiez que l'agent SSM s'exécute sur l'instance EC2 et qu'une association a été créée pour collecter l'inventaire des logiciels d'applications. La règle renvoie NOT_APPLICABLE si l'agent SSM n'est pas installé ou si aucune association n'a été créée ou ne s'exécute.

Identificateur : EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Types de ressources : AWS::SSM::ManagedInstance Inventaire

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

applicationNames, Type : CSV

Liste de noms d'applications séparés par des virgules. Si vous le souhaitez, spécifiez les versions ajoutées avec « : » (par exemple, « Chrome : 0.5.3, FireFox »).

> **Note**
>
> Les noms d'applications doivent être des correspondances exactes. Par exemple, utilisez **`firefox`** sous Linux ou **`firefox-compat`** sous Amazon Linux. En outre, AWS Config ne prend actuellement pas en charge les caractères génériques pour le paramètre ApplicationNames (par exemple,). **`firefox*`**

platformType (facultatif), Type : chaîne

Type de plateforme (par exemple, « Linux » ou « Windows »).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-managedinstance-association-compliance-status-check

Vérifie si le statut de conformité de l'association AWS Systems Manager est COMPLIANT ou NON_COMPLIANT après l'exécution de l'association sur l'instance. La règle est conforme si le champ contient l'état COMPLIANT. Pour plus d'informations sur les associations, consultez Qu'est-ce qu'une association ?.

Identificateur : EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

Types de ressources : AWS::SSM::AssociationCompliance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-managedinstance-inventory-blacklisted

Vérifie si les instances gérées par Amazon EC2 Systems Manager sont configurées pour collecter les types d'inventaire sur liste noire.

Identificateur : EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Types de ressources : AWS::SSM::ManagedInstance Inventaire

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

inventoryNames, Type : CSV

Liste des types d'inventaire de Systems Manager séparés par des virgules (par exemple, « :Network AWS, : AWS »). WindowsUpdate

platformType (facultatif), Type : chaîne

Type de plateforme (par exemple, « Linux »).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-managedinstance-patch-compliance-status-check

Vérifie si l'état de conformité du correctif de AWS Systems Manager est CONFORME ou NON_COMPLIANT après l'installation du correctif sur l'instance. La règle est conforme si le champ contient l'état COMPLIANT.

Identificateur : EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

Types de ressources : AWS::SSM::PatchCompliance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ec2-managedinstance-platform-check

Vérifie si les instances gérées EC2 présentent les configurations souhaitées.

Identificateur : EC2_MANAGEDINSTANCE_PLATFORM_CHECK

Types de ressources : AWS::SSM::ManagedInstance Inventaire

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

platformType, Type : chaîne

Type de plateforme (par exemple, « Linux »).

platformVersion (facultatif), Type : chaîne

Version de plateforme (par exemple, « 2016.09 »).

agentVersion (facultatif), Type : chaîne

Version de l'agent (par exemple « 2.0.433.0 »).

platformName (facultatif), Type : chaîne

Version de la plateforme (par exemple, « 2016.09 »)

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ec2-meets-restore-time-target

Vérifie si la durée de restauration des instances Amazon Elastic Compute Cloud (Amazon EC2) est conforme à la durée spécifiée. La règle est NON_COMPLIANT si la durée LatestRestoreExecutionTimeMinutes d'une instance Amazon EC2 est supérieure à quelques minutes. maxRestoreTime

Identifiant : EC2_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::EC2::Instance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balise des instances Amazon EC2 pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

ID de l'instance Amazon EC2 pour la règle à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-no-amazon-key-pair

Vérifie si les instances Amazon Elastic Compute Cloud (EC2) en cours d'exécution sont lancées à l'aide des paires de clés Amazon. La règle est NON_COMPLIANT si une instance EC2 en cours d'exécution est lancée avec une paire de clés.

Identificateur : EC2_NO_AMAZON_KEY_PAIR

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-paravirtual-instance-check

Vérifie si la virtualisation d'une instance EC2 est de type paravirtuel. Cette règle est NON_COMPLIANT pour une instance EC2 si « VirtualizationType » est défini sur « paravirtual ».

Identificateur : EC2_PARAVIRTUAL_INSTANCE_CHECK

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Chine (Beijing), Europe (Irlande), Europe (Francfort), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Tokyo),

USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-resources-protected-by-backup-plan

Vérifie si les instances Amazon Elastic Compute Cloud (Amazon EC2) sont protégées par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué à l'instance Amazon EC2.

> **Note**
>
> Cette règle s'applique uniquement aux instances Amazon EC2 en cours d'exécution et non aux instances arrêtées.

Identificateur : EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::EC2::Instance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balise des instances Amazon EC2 pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID de l'instance Amazon EC2 pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-security-group-attached-to-eni

Vérifie si les groupes de sécurité qui ne sont pas configurés par défaut sont associés aux interfaces réseau élastiques. La règle est NON_COMPLIANT si le groupe de sécurité n'est pas associé à une interface réseau.

Identificateur : EC2_SECURITY_GROUP_ATTACHED_TO_ENI

Types de ressources : AWS::EC2::SecurityGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-security-group-attached-to-eni-periodic

Vérifie si les groupes de sécurité qui ne sont pas configurés par défaut sont associés aux interfaces réseau Elastic (ENI). La règle est NON_COMPLIANT si le groupe de sécurité n'est pas associé à une ENI. Les groupes de sécurité n'appartenant pas au compte appelant sont considérés comme NOT_APPLICABLE.

> **Note**
>
> Cette règle rend compte sur le type de ressource `AWS::EC2::SecurityGroup`. Toutefois, pour le bon fonctionnement de la règle, vous devez activer l'enregistrement du type de ressource `AWS::EC2::NetworkInterface`.

Identificateur : EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

Types de ressources : AWS::EC2::SecurityGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-stopped-instance

Vérifie si des instances Amazon Elastic Compute Cloud (Amazon EC2) sont arrêtées plus longtemps que le nombre de jours autorisé. La règle est NON_COMPLIANT si l'état d'une instance Amazon EC2

a été arrêté plus longtemps que le nombre de jours autorisé ou si la durée de l'arrêt ne peut être déterminée.

Identificateur : EC2_STOPPED_INSTANCE

Types de ressources : AWS::EC2::Instance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

AllowedDays (Facultatif), Type : int, Valeur par défaut : 30

Le nombre de jours pendant lesquels une instance Amazon EC2 peut être arrêtée avant que la règle ne soit NON_COMPLIANT. Le nombre de jours par défaut est 30.

> **Note**
>
> Le nombre de jours sélectionnés doit être inférieur à la période de conservation configurée car cette règle repose sur les données historiques collectées. Pour plus d'informations sur la conservation des données historiques, consultez la section Suppression AWS Config de données.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-token-hop-limit-check

Vérifie si les métadonnées d'une instance Amazon Elastic Compute Cloud (EC2) présentent une limite de sauts de jetons spécifiée qui est inférieure à la limite souhaitée. La règle est NON_COMPLIANT pour une instance si elle présente une valeur limite de sauts supérieure à la limite prévue.

Identificateur : EC2_TOKEN_HOP_LIMIT_CHECK

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

tokenHopLimit (Facultatif), Type : int

Limite de sauts de jetons souhaitée. Les valeurs valides sont comprises entre 1 et 64, les deux inclus. La valeur par défaut est 1 si aucune valeur n'est spécifiée.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-transit-gateway-auto-vpc-attach-disabled

Vérifie si « » est activé sur les passerelles de transit Amazon Elastic Compute Cloud (Amazon EC2). AutoAccept SharedAttachments La règle est NON_COMPLIANT pour un Transit Gateway si « AutoAccept SharedAttachments » est défini sur « activer ».

Identificateur : EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

Types de ressources : AWS::EC2::TransitGateway

Type de déclencheur : changements de configuration

Région AWS: Disponible uniquement en Europe (Stockholm), Europe (Paris), USA Est (Ohio), Afrique (Le Cap), Europe (Irlande), Europe (Francfort), Amérique du Sud (Sao Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Europe (Milan), Asie-Pacifique (Tokyo), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney)), Région du Canada (Centre)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-volume-inuse-check

Vérifie si les volumes EBS sont associés à des instances EC2. Vérifie éventuellement si les volumes EBS sont marqués pour suppression lorsqu'une instance est mise hors service.

La règle est COMPLIANT si un volume EBS est associé à une instance EC2 en cours d'exécution. Dans ce cas, elle est COMPLIANT lorsque le volume EBS est activement utilisé par une instance EC2.

La règle est NON_COMPLIANT si un volume EBS n'est associé à aucune instance EC2 ou s'il est associé à une instance EC2 arrêtée ou mise hors service. Dans ce cas, elle est NON_COMPLIANT lorsque le volume EBS n'est pas activement utilisé par une instance EC2.

Identificateur : EC2_VOLUME_INUSE_CHECK

Types de ressources : AWS::EC2::Volume

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

deleteOnTermination (Facultatif), Type : valeur booléenne

> Les volumes EBS sont marqués pour suppression lorsqu'une instance est mise hors service. Valeurs possibles : True ou False (les autres valeurs d'entrée sont marquées comme NON_COMPLIANT). Si elle est définie sur `True`, la règle est NON_COMPLIANT si un volume EBS mis hors service n'est pas marqué pour suppression.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ecr-private-image-scanning-enabled

Vérifie si la numérisation d'images est activée dans un référentiel privé Amazon Elastic Container Registry (Amazon ECR). La règle est NON_COMPLIANT si la fréquence d'analyse du référentiel Amazon ECR privé n'est pas définie sur l'analyse lors du transfert ou l'analyse continue. Pour plus

d'informations sur l'activation de la numérisation d'images, consultez Numérisation d'images dans le Guide de l'utilisateur Amazon ECR.

Identificateur : ECR_PRIVATE_IMAGE_SCANNING_ENABLED

Types de ressources : AWS::ECR::Repository

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecr-private-lifecycle-policy-configured

Vérifie si au moins une politique de cycle de vie est configurée dans un référentiel privé Amazon Elastic Container Registry (ECR). La règle est NON_COMPLIANT si aucune politique de cycle de vie n'est configurée pour le référentiel ECR privé.

Identificateur : ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

Types de ressources : AWS::ECR::Repository

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecr-private-tag-immutability-enabled

Vérifie si l'immuabilité des balises est activée dans un référentiel privé Amazon Elastic Container Registry (ECR). Cette règle est NON_COMPLIANT si l'immuabilité des balises n'est pas activée pour le référentiel ECR privé.

Identificateur : ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

Types de ressources : AWS::ECR::Repository

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ecs-awsvpc-networking-enabled

Vérifie si le mode réseau pour l'ECS actif TaskDefinitions est défini sur « awsvpc ». Cette règle est NON_COMPLIANT si l'ECS actif n'TaskDefinitions est pas défini sur « awsvpc ».

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identifiant : AWSVPC_NETWORKING ECS_ _ENABLED

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecs-containers-nonprivileged

Vérifie si le paramètre privilégié dans la définition du conteneur d'ECS TaskDefinitions est défini sur « vrai ». La règle est NON_COMPLIANT si le paramètre privilégié est défini sur « true ».

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identificateur : ECS_CONTAINERS_NONPRIVILEGED

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecs-containers-readonly-access

Vérifie si les conteneurs Amazon Elastic Container Service (Amazon ECS) disposent d'un accès en lecture seule au niveau de leurs systèmes de fichiers racine. La règle est NON_COMPLIANT si le

readonlyRootFilesystem paramètre de la définition du conteneur d'ECS TaskDefinitions est défini sur « false ».

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identificateur : ECS_CONTAINERS_READONLY_ACCESS

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ecs-container-insights-enabled

Vérifie si les informations sur les conteneurs sont activées sur les clusters Amazon Elastic Container Service. La règle est NON_COMPLIANT si les instances de conteneur ne sont pas activées.

Identificateur : ECS_CONTAINER_INSIGHTS_ENABLED

Types de ressources : AWS::ECS::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecs-fargate-latest-platform-version

Vérifie si les services ECS Fargate sont configurés avec la dernière version de plateforme. La règle est NON_COMPLIANT si, PlatformVersion pour le Fargate, le type de lancement n'est pas défini sur LATEST, ou si aucun latestLinuxVersion des deux n'est fourni en tant que paramètre. `latestWindowsVersion`

Identificateur : ECS_FARGATE_LATEST_PLATFORM_VERSION

Types de ressources : AWS::ECS::Service

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

latestLinuxVersion (Facultatif), Type : chaîne

La dernière version de Linux PlatformVersion supportait « » au format sémantique de version (SemVer). Le paramètre peut être nécessaire si Fargate a été déployé et que le PlatformVersion « » a été explicitement spécifié CodeDeploy ou est utilisé comme « » DeploymentController

latestWindowsVersion (Facultatif), Type : chaîne

La dernière version de Windows PlatformVersion supportait « » au format de version sémantique (SemVer). Le paramètre peut être nécessaire si Fargate a été déployé et que le PlatformVersion « » a été explicitement spécifié CodeDeploy ou est utilisé comme « » DeploymentController

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecs-no-environment-secrets

Vérifie si les secrets sont transmis en tant que variables d'environnement de conteneur. La règle est NON_COMPLIANT si une ou plusieurs clés de variable d'environnement correspondent à une clé répertoriée dans le paramètre « `secretKeys` » (à l'exception des variables environnementales provenant d'autres emplacements tels qu'Amazon S3).

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identificateur : ECS_NO_ENVIRONMENT_SECRETS

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

secretKeys, Type : CSV

Liste de noms de clés séparés par des virgules, permettant d'effectuer des recherches dans les variables d'environnement des définitions de conteneurs dans les définitions de tâches. Les espaces supplémentaires seront supprimés.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ecs-task-definition-log-configuration

Vérifie si logConfiguration est défini sur les définitions de tâches ECS actives. Cette règle est NON_COMPLIANT si la ressource LogConfiguration TaskDefinition n'est pas définie pour un ECS actif ou si la valeur de LogConfiguration est nulle dans au moins une définition de conteneur.

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identificateur : ECS_TASK_DEFINITION_LOG_CONFIGURATION

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ecs-task-definition-memory-hard-limit

Vérifie si les définitions des tâches Amazon Elastic Container Service (ECS) présentent une limite de mémoire définie pour leurs définitions de conteneurs. La règle est NON_COMPLIANT pour une définition de tâche si le paramètre « memory » est absent dans une définition de conteneur.

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identificateur : ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecs-task-definition-nonroot-user

Vérifie si ECS TaskDefinitions spécifie un utilisateur pour les conteneurs de type lancement Amazon Elastic Container Service (Amazon ECS) EC2 sur lesquels s'exécuter. La règle est NON_COMPLIANT si le paramètre « user » est absent ou s'il est défini sur « root ».

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identificateur : ECS_TASK_DEFINITION_NONROOT_USER

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ecs-task-definition-pid-mode-check

Vérifie si ECS TaskDefinitions est configuré pour partager l'espace de noms de processus d'un hôte avec ses conteneurs Amazon Elastic Container Service (Amazon ECS). La règle est NON_COMPLIANT si le paramètre pidMode est défini sur « host ».

> **Note**
>
> Cette règle évalue uniquement la dernière révision active d'une définition de tâche Amazon ECS.

Identificateur : ECS_TASK_DEFINITION_PID_MODE_CHECK

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

ecs-task-definition-user-for-host-mode-check

Vérifie les autorisations non autorisées dans les dernières définitions de tâches actives Amazon Elastic Container Service (Amazon ECS), dans lesquelles `NetworkMode` est défini sur host. La règle est NON_COMPLIANT pour les définitions de tâches dans lesquelles `NetworkMode` est défini sur host et les définitions de conteneur où `privileged` est défini sur false ou empty, et `user` est défini sur root ou empty.

> **Important**
>
> Nous vous recommandons de supprimer les privilèges élevés des définitions de tâches Amazon ECS. Lorsque `privileged` c'est vrai, le conteneur reçoit des autorisations élevées

sur l'instance du conteneur hôte (similaire à l'`root`utilisateur). Lorsque vous exécutez des tâches en mode réseau `host`, vous n'exécutez pas de conteneurs à l'aide de l'utilisateur root (UID 0) pour une meilleure sécurité. Comme bonne pratique de sécurité, utilisez toujours un utilisateur non root.

Identificateur : ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Types de ressources : AWS::ECS::TaskDefinition

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

SkipInactiveTaskDefinitions (Facultatif), Type : valeur booléenne

Indicateur booléen permettant de ne pas vérifier les définitions de tâches Amazon EC2 INACTIVES. Si elle est définie sur « true », la règle n'évaluera pas les définitions de tâches Amazon EC2 INACTIVES. Si elle est définie sur « false », la règle évaluera la dernière révision des définitions de tâches Amazon EC2 INACTIVES.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

efs-access-point-enforce-root-directory

Vérifie si les points d'accès Amazon Elastic File System (Amazon EFS) sont configurés pour appliquer un répertoire racine. La règle est NON_COMPLIANT si la valeur de « Path » est définie sur «/» (répertoire racine par défaut du système de fichiers).

Identificateur : EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Types de ressources : AWS::EFS::AccessPoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

approvedDirectories (facultatif), Type : CSV

Liste de chemins de sous-répertoires approuvés pour l'application de répertoire racine des points d'accès Amazon EFS, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

efs-access-point-enforce-user-identity

Vérifie si les points d'accès Amazon Elastic File System (Amazon EFS) sont configurés pour appliquer une identité utilisateur. La règle est NON_COMPLIANT si « PosixUser » n'est pas défini ou si des paramètres sont fournis et que le paramètre correspondant ne correspond pas.

Identificateur : EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

Types de ressources : AWS::EFS::AccessPoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

approvedUids (facultatif), Type : CSV

Liste d'ID d'utilisateur POSIX approuvés pour l'application de points d'accès EFS par les utilisateurs, séparés par des virgules.

approvedGids (facultatif), Type : CSV

Liste d'ID de groupe POSIX approuvés pour l'application de points d'accès EFS par les utilisateurs, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

efs-encrypted-check

Vérifie si Amazon Elastic File System (Amazon EFS) est configuré pour chiffrer les données du fichier à l'aide de AWS Key Management Service (AWS KMS). La règle est NON_COMPLIANT si la clé chiffrée est définie sur false sur `DescribeFileSystems` ou si la clé `KmsKeyId` sur `DescribeFileSystems` ne correspond pas au paramètre `KmsKeyId`.

Identificateur : EFS_ENCRYPTED_CHECK

Types de ressources : AWS::EFS::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

KmsKeyId (Facultatif), Type : chaîne

Amazon Resource Name (ARN) de la clé KMS utilisée pour chiffrer le système de fichiers EFS.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

efs-in-backup-plan

Vérifie si les systèmes de fichiers Amazon Elastic File System (Amazon EFS) sont ajoutés dans les plans de sauvegarde de AWS Backup. La règle est NON_COMPLIANT si aucun système de fichiers EFS n'est inclus dans les plans de sauvegarde.

Identificateur : EFS_IN_BACKUP_PLAN

Types de ressources : AWS::EFS::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

efs-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour les systèmes de fichiers Amazon Elastic File System (Amazon EFS). La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans le système de fichiers Amazon EFS.

Identificateur : EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::EFS::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balise des systèmes de fichiers EFS pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du système de fichiers EFS pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

efs-meets-restore-time-target

Vérifie si la durée de restauration des systèmes de fichiers Amazon Elastic File System (Amazon EFS) est conforme à la durée spécifiée. La règle est NON_COMPLIANT si la durée LatestRestoreExecutionTimeMinutes d'un système de fichiers Amazon EFS est supérieure maxRestoreTime à quelques minutes.

Identifiant : EFS_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::EFS::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balise des systèmes de fichiers EFS pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

ID du système de fichiers EFS pour la règle à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

efs-mount-target-accessible au public

Vérifie si une cible de montage Amazon Elastic File System (Amazon EFS) n'est pas associée à un sous-réseau public. La règle n'est PAS CONFORME si la cible de montage Amazon EFS est associée à un sous-réseau public.

Identifiant : EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

Types de ressources : AWS::EFS::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

efs-resources-protected-by-backup-plan

Vérifie si les systèmes de fichiers Amazon Elastic File System (Amazon EFS) sont protégés par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué au système de fichiers EFS.

Identificateur : EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::EFS::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balise des systèmes de fichiers EFS pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du système de fichiers EFS pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eip-attached

Vérifie si toutes les adresses IP élastiques attribuées à un AWS compte sont associées à des instances EC2 ou à des interfaces réseau élastiques en cours d'utilisation. La règle est NON_COMPLIANT si le « AssociationId » est nul pour l'adresse IP élastique.

> **Note**
>
> Il faut parfois attendre jusqu'à 6 heures pour connaître les résultats d'une évaluation.

Identificateur : EIP_ATTACHED

Types de ressources : AWS::EC2::EIP

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eks-cluster-logging-enabled

Vérifie si la journalisation est activée sur un cluster Amazon Elastic Kubernetes Service (Amazon EKS). La règle est NON_COMPLIANT si la journalisation des clusters Amazon EKS n'est pas activée pour tous les types de journaux.

Identificateur : EKS_CLUSTER_LOGGING_ENABLED

Types de ressources : AWS::EKS::Cluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eks-cluster-log-enabled

Vérifie si la journalisation est activée sur un cluster Amazon Elastic Kubernetes Service (Amazon EKS). La règle est NON_COMPLIANT si la journalisation des clusters Amazon EKS n'est pas activée ou si la journalisation n'est pas activée avec le type de journal mentionné.

Identificateur : EKS_CLUSTER_LOG_ENABLED

Types de ressources : AWS::EKS::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

logTypes (facultatif), Type : CSV

Liste de types de journaux de plan de contrôle du cluster EKS qui doivent être activés, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eks-cluster-oldest-supported-version

Vérifie si un cluster Amazon Elastic Kubernetes Service (EKS) exécute la plus ancienne version prise en charge. La règle est NON_COMPLIANT si un cluster EKS exécute la plus ancienne version prise en charge (égale au paramètre « `oldestVersionSupported` »).

Identificateur : EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

Types de ressources : AWS::EKS::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

le plus vieux VersionSupported, Type : chaîne

Valeur de la plus ancienne version de Kubernetes prise en charge sur AWS.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eks-cluster-secrets-encrypted

Vérifie si les clusters Amazon EKS sont configurés pour que les secrets Kubernetes soient chiffrés à l'aide de KMS. AWS La règle est NON_COMPLIANT si un cluster EKS ne possède pas de ressource EncryptionConfig ou si EncryptionConfig ne nomme pas les secrets en tant que ressource.

Identifiant : EKS_CLUSTER_SECRETS_ENCRYPTED

Types de ressources : AWS::EKS::Cluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

Liste séparée par des virgules des noms de ressources Amazon (ARN) clés KMS approuvés pour l'utilisation d'EKS.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eks-cluster-supported-version

Vérifie si un cluster Amazon Elastic Kubernetes Service (EKS) exécute une version Kubernetes prise en charge. Cette règle est NON_COMPLIANT si un cluster EKS exécute une version non prise en charge (inférieure au paramètre «`oldestVersionSupported`»).

Identificateur : EKS_CLUSTER_SUPPORTED_VERSION

Types de ressources : AWS::EKS::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

le plus vieux VersionSupported, Type : chaîne

Valeur de la plus ancienne version de Kubernetes prise en charge sur AWS.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eks-endpoint-no-public-access

Vérifie si le point de terminaison Amazon Elastic Kubernetes Service (Amazon EKS) n'est pas publiquement accessible. La règle est NON_COMPLIANT si le point de terminaison est publiquement accessible.

Identificateur : EKS_ENDPOINT_NO_PUBLIC_ACCESS

Types de ressources : AWS::EKS::Cluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

eks-secrets-encrypted

Vérifie si les clusters Amazon Elastic Kubernetes Service sont configurés pour que les secrets Kubernetes soient chiffrés à l'aide de clés (KMS). AWS Key Management Service

- Cette règle est COMPLIANT si un paramètre encryptionConfig est appliqué à un cluster EKS et si l'une des ressources de ce paramètre comprend les secrets.
- Cette règle est également COMPLIANT si la clé utilisée pour chiffrer les secrets EKS correspond au paramètre.
- Cette règle est NON_COMPLIANT si aucun paramètre encryptionConfig n'est appliqué à un cluster EKS ou si les ressources EncryptionConfig n'incluent pas de secrets.
- Cette règle est également NON_COMPLIANT si la clé utilisée pour chiffrer les secrets EKS ne correspond pas au paramètre.

Identificateur : EKS_SECRETS_ENCRYPTED

Types de ressources : AWS::EKS::Cluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

> Liste d'Amazon Resource Name (ARN) de la clé KMS devant être utilisée pour les secrets chiffrés dans un cluster EKS, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

elasticache-auto-minor-version-upgrade-check

Vérifie si les mises ElastiCache à niveau automatiques des versions mineures des clusters Amazon pour Redis sont activées. La règle est NON_COMPLIED pour un ElastiCache cluster s'il utilise le moteur Redis et si « » n'est pas défini sur AutoMinor VersionUpgrade « vrai ».

Identificateur : ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

Types de ressources : AWS::ElastiCache::CacheCluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticache-rbac-auth-enabled

Vérifie si l'authentification RBAC est activée pour les groupes de ElastiCache réplication Amazon. La règle est NON_COMPLIED si la version de Redis est 6 ou supérieure et que « UserGroup Ids » est manquant, vide ou ne correspond pas à une entrée fournie par le paramètre « ». `allowedUserGroupIDs`

Identificateur : ELASTICACHE_RBAC_AUTH_ENABLED

Types de ressources : AWS::ElastiCache::ReplicationGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

UserGroupidentifiants autorisés (facultatif), Type : CSV

> Liste séparée par des virgules des identifiants de groupes d'utilisateurs approuvés pour l'accès aux groupes de ElastiCache réplication.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticache-redis-cluster-automatic-backup-check

Vérifiez si la sauvegarde automatique ElastiCache est activée sur les clusters Amazon Redis. La règle est NON_COMPLIANT si le cluster SnapshotRetentionLimit for Redis est inférieur au paramètre. SnapshotRetentionPeriod Par exemple : si le paramètre est 15, la règle n'est pas conforme si elle snapshotRetentionPeriod est comprise entre 0 et 15.

Identificateur : ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

Types de ressources : AWS::ElastiCache::CacheCluster, AWS::ElastiCache::ReplicationGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

snapshotRetentionPeriod (Facultatif), Type : int, Valeur par défaut : 15

> Période de conservation minimale d'instantané en jours pour le cluster Redis. La valeur par défaut est de 15 jours.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

elasticache-repl-grp-auto-failover-enabled

Vérifie si le basculement automatique ElastiCache est activé pour les groupes de réplication Amazon Redis. La règle est NON_COMPLIANT pour un groupe de ElastiCache réplication si « AutomaticFailover » n'est pas défini sur « activé ».

Identificateur : ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

Types de ressources : AWS::ElastiCache::ReplicationGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticache-repl-grp-encrypted-at-rest

Vérifie si les groupes ElastiCache de réplication Amazon sont encryption-at-rest activés. La règle est NON_COMPLIANT pour un groupe de ElastiCache réplication si « AtRest EncryptionEnabled » est désactivé ou si l'ARN de la clé KMS ne correspond pas au paramètre KeyArns ApprovedKMS.

Identificateur : ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

Types de ressources : AWS::ElastiCache::ReplicationGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

KMS approuvés KeyIds (facultatif), Type : CSV

Liste séparée par des virgules des identifiants de clé KMS dont l'utilisation est approuvée. ElastiCache

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticache-repl-grp-encrypted-in-transit

Vérifie si les groupes ElastiCache de réplication Amazon sont encryption-in-transit activés. La règle est NON_COMPLIANT pour un groupe de ElastiCache réplication si « TransitEncryption Enabled » est défini sur « false ».

Identificateur : ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

Types de ressources : AWS::ElastiCache::ReplicationGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticache-repl-grp-redis-auth-enabled

Vérifie si Redis AUTH est activé sur les groupes de ElastiCache réplication Amazon. La règle est NON_COMPLIED pour un groupe de ElastiCache réplication si la version Redis de ses nœuds est inférieure à 6 (les versions 6+ utilisent des ACL Redis) et si « AuthToken » est manquant ou est vide/nul.

Identificateur : ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

Types de ressources : AWS::ElastiCache::ReplicationGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticache-subnet-group-check

Vérifie si les ElastiCache clusters Amazon sont configurés avec un groupe de sous-réseaux personnalisé. La règle est NON_COMPLIANT pour un ElastiCache cluster s'il utilise un groupe de sous-réseaux par défaut.

Identificateur : ELASTICACHE_SUBNET_GROUP_CHECK

Types de ressources : AWS::ElastiCache::CacheCluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticache-supported-engine-version

Vérifie si les ElastiCache clusters exécutent une version supérieure ou égale à la version du moteur recommandée. La règle est NON_COMPLIANT si le « EngineVersion » d'un ElastiCache cluster est inférieur à la version recommandée spécifiée pour le moteur donné.

Identificateur : ELASTICACHE_SUPPORTED_ENGINE_VERSION

Types de ressources : AWS::ElastiCache::CacheCluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

le plus récent MemcachedVersion, Type : chaîne

Dernière version de moteur recommandée pour Memcached. Les valeurs valides sont au format de versionnement sémantique (SemVer) avec un numéro à 3 composants pour les versions majeures, mineures et correctifs (par exemple, 1.6.6, pas 1.6).

le plus récent RedisVersion, Type : chaîne

Dernière version de moteur recommandée pour Redis. Les valeurs valides sont au format de versionnement sémantique (SemVer) avec un numéro à 3 composants pour les versions majeures, mineures et correctifs (par exemple, 7.0.5, pas 7.0).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticsearch-encrypted-at-rest

Vérifie si la configuration du chiffrement au repos est activée dans les domaines Amazon OpenSearch Service (précédemment appelés Elasticsearch). La règle est NON_COMPLIANT si le EncryptionAtRestOptions champ n'est pas activé.

Identificateur : ELASTICSEARCH_ENCRYPTED_AT_REST

Types de ressources : AWS::Elasticsearch::Domain

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticsearch-in-vpc-only

Vérifie si les domaines Amazon OpenSearch Service (anciennement Elasticsearch) se trouvent dans Amazon Virtual Private Cloud (Amazon VPC). La règle est NON_COMPLIANT si un point de terminaison OpenSearch du domaine de service est public.

Identificateur : ELASTICSEARCH_IN_VPC_ONLY

Types de ressources : AWS::Elasticsearch::Domain

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticsearch-logs-to-cloudwatch

Vérifie si les domaines Amazon OpenSearch Service sont configurés pour envoyer des journaux à Amazon CloudWatch Logs. La règle est COMPLIANT si un journal est activé pour un domaine Amazon ES. Cette règle est NON_COMPLIANT si la journalisation n'est pas configurée.

Identificateur : ELASTICSEARCH_LOGS_TO_CLOUDWATCH

Types de ressources : AWS::Elasticsearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

logTypes (facultatif), Type : CSV

Liste des journaux activés, séparés par des virgules. Les valeurs valides sont « search », « index » et « error ».

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*Objet doté d'une ou plusieurs des clés suivantes : `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS`, `AUDIT_LOGS`, selon les types de journaux que vous souhaitez publier. Chaque clé a besoin d'une valeur `LogPublishingOption` valide.

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elasticsearch-node-to-node-encryption-check

Vérifiez si les nœuds OpenSearch du service (précédemment appelés Elasticsearch) sont chiffrés de bout en bout. La règle est NON_COMPLIANT si le node-to-node chiffrement n'est pas activé sur le domaine.

Identificateur : ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Types de ressources : AWS::Elasticsearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
```

```
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elastic-beanstalk-logs-to-cloudwatch

Vérifie si les environnements AWS Elastic Beanstalk sont configurés pour envoyer des journaux à Amazon Logs. CloudWatch La règle est NON_COMPLIANT si la valeur de `StreamLogs` est fausse.

Identificateur : ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

Types de ressources : AWS::ElasticBeanstalk::Environment

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

RetentionInDays (Facultatif), Type : chaîne

> Vérifie le nombre de jours pendant lesquels les événements de journal doivent être conservés avant leur expiration. Les valeurs possibles sont : 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 et 3653. La règle est NON_COMPLIANT s'il s'agit de la valeur de `logs. RetentionInDays` ne correspond pas à ce paramètre.

DeleteOnTerminate (Facultatif), Type : chaîne

> Vérifie si les journaux sont configurés pour être supprimés lors de la mise hors service de l'environnement. Les valeurs valides sont « true » ou « false ». La règle est NON_COMPLIANT s'il s'agit de la valeur de `logs. DeleteOnTerminate` ne correspond pas à ce paramètre.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elastic-beanstalk-managed-updates-enabled

Vérifie si les mises à jour de plateforme gérées dans un AWS Elastic Beanstalk environnement sont activées. La règle est COMPLIANT si la valeur de `ManagedActionsEnabled` est définie sur true. La règle est NON_COMPLIANT si la valeur de `ManagedActionsEnabled` est définie sur false ou si un paramètre dont la valeur ne correspond pas aux configurations existantes est fourni.

Identificateur : ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

Types de ressources : AWS::ElasticBeanstalk::Environment

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

UpdateLevel (Facultatif), Type : chaîne

> Indique si les niveaux de mise à jour sont définis sur des mises à jour de version « minor » ou sur des mises à jour de version « patch ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

elbv2-acm-certificate-required

Vérifie si les équilibreurs de charge d'application et les équilibreurs de charge réseau disposent d'écouteurs configurés pour utiliser des certificats provenant de AWS Certificate Manager (ACM). Cette règle est NON_COMPLIANT si au moins un équilibreur de charge présente au moins un écouteur configuré sans un certificat ACM ou configuré avec un certificat qui ne provient pas d'ACM.

Identificateur : ELBV2_ACM_CERTIFICATE_REQUIRED

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

AcmCertificatesAllowed (Facultatif), Type : CSV

Liste d'Amazon Resource Names (ARN) séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elbv2-multiple-az

Vérifie si un Elastic Load Balancer V2 (Application, Network, ou Gateway Load Balancer) est mappé à plusieurs zones de disponibilité (AZ). La règle est NON_COMPLIANT si un Elastic Load Balancer V2 est mappé à moins de 2 AZ. Pour plus d'informations, consultez Zones de disponibilité pour votre Application Load Balancer.

Identificateur : ELBV2_MULTIPLE_AZ

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

minAvailabilityZones (Facultatif), Type : int

Nombre minimal d'AZ attendues (entre 2 et 10 inclus).

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elb-acm-certificate-required

Vérifie si les équilibreurs de charge classiques utilisent les certificats SSL fournis par AWS Certificate Manager. Pour vous servir de cette règle, utilisez un écouteur SSL ou HTTPS avec votre Classic

Load Balancer. Cette règle s'applique uniquement aux Classic Load Balancers. Cette règle ne vérifie pas les Application Load Balancers, ni les Network Load Balancers.

Identificateur : ELB_ACM_CERTIFICATE_REQUIRED

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elb-cross-zone-load-balancing-enabled

Vérifie si l'équilibrage de charge entre zones est activé sur les Classic Load Balancers. La règle est NON_COMPLIANT si l'équilibrage de charge entre zones n'est pas activé sur les Classic Load Balancers.

Identificateur : ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elb-custom-security-policy-ssl-check

Vérifie si les écouteurs SSL de votre Classic Load Balancer utilisent une politique personnalisée. La règle est applicable uniquement si le Classic Load Balancers est associé à des écouteurs SSL.

Identificateur : ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

ProtocolsAndChiffrements SSL, Type : chaîne

Liste de chiffrements et de protocoles, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, consultez[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

elb-deletion-protection-enabled

Vérifie si la protection contre la suppression est activée sur un Elastic Load Balancer. La règle est NON_COMPLIANT si deletion_protection.enabled est défini sur false.

Identificateur : ELB_DELETION_PROTECTION_ENABLED

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elb-logging-enabled

Vérifie si la journalisation est activée pour Application Load Balancer et Classic Load Balancer. La règle est NON_COMPLIANT si elle `access_logs.s3.enabled` est fausse ou n'`access_logs.S3.bucket`est pas égale à la valeur s3 BucketName que vous avez fournie.

> **Note**
>
> La règle ne s'applique pas aux Network Load Balancers ni aux Gateway Load Balancers.

Identificateur : ELB_LOGGING_ENABLED

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

s3 BucketNames (facultatif), Type : CSV

Liste de noms de compartiment Amazon S3 séparés par des virgules permettant à Amazon ELB de fournir les fichiers journaux.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elb-predefined-security-policy-ssl-check

Vérifie si les écouteurs SSL Classic Load Balancer utilisent une politique prédéfinie. La règle est NON_COMPLIANT si la politique de l'écouteur HTTPS/SSL Classic Load Balancer n'est pas égale à la valeur du paramètre « `predefinedPolicyName` ».

Identificateur : ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

prédéfini PolicyName, Type : chaîne

Nom de la politique prédéfinie.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

elb-tls-https-listeners-only

Vérifie si votre Classic Load Balancer est configuré avec des écouteurs SSL ou HTTPS. La règle est NON_COMPLIANT si un écouteur n'est pas configuré avec SSL ou HTTPS.

- Si aucun écouteur n'est configuré pour le Classic Load Balancer, la règle renvoie NOT_APPLICABLE.
- La règle est COMPLIANT si les écouteurs Classic Load Balancer sont configurés avec SSL ou HTTPS.
- La règle est NON_COMPLIANT si un écouteur n'est pas configuré avec SSL ou HTTPS.

Identificateur : ELB_TLS_HTTPS_LISTENERS_ONLY

Types de ressources : AWS::ElasticLoadBalancing::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

emr-block-public-access

Vérifie si les paramètres de blocage de l'accès public sont activés sur un compte Amazon EMR. La règle est NON_COMPLIANT si elle BlockPublicSecurityGroupRules est fausse, ou si elle est vraie, les ports autres que le port 22 sont répertoriés dans. PermittedPublicSecurityGroupRuleRanges

Identificateur : EMR_BLOCK_PUBLIC_ACCESS

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

emr-kerberos-enabled

Vérifie si Kerberos est activé sur les clusters Amazon EMR. La règle est NON_COMPLIANT si une configuration de sécurité n'est pas attachée au cluster ou si la configuration de sécurité ne satisfait pas aux paramètres de règle spécifiés.

Identificateur : EMR_KERBEROS_ENABLED

Types de ressources : AWS::EMR::Cluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

TicketLifetimeInHours (Facultatif), Type : int

Période pendant laquelle le ticket Kerberos émis par le KDC du cluster est valide.

Realm (facultatif), Type : chaîne

Nom de domaine Kerberos de l'autre domaine inclus dans la relation d'approbation.

Domain (facultatif), Type : chaîne

Nom de domaine de l'autre domaine de la relation d'approbation.

AdminServer (Facultatif), Type : chaîne

Nom de domaine complet du serveur d'administration de l'autre domaine inclus dans la relation d'approbation.

KdcServer (Facultatif), Type : chaîne

Nom de domaine complet du serveur KDC de l'autre domaine inclus dans la relation d'approbation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

emr-master-no-public-ip

Vérifie si les nœuds principaux des clusters Amazon EMR présentent des adresses IP publiques. La règle est NON_COMPLIANT si le nœud principal a une adresse IP publique.

> **Note**
>
> Cette règle vérifie les clusters à l'état RUNNING ou WAITING. Cette règle exige que vous activiez l'enregistrement pour le type de ressource `AWS::EC2::Instance` afin d'obtenir une évaluation précise.

Identificateur : EMR_MASTER_NO_PUBLIC_IP

Types de ressources : AWS::EMR::Cluster, AWS::EC2::Instance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

encrypted-volumes

Vérifie si les volumes Amazon EBS associés sont chiffrés et sont éventuellement chiffrés avec une clé KMS spécifiée. La règle est NON_COMPLIANT si les volumes EBS associés ne sont pas chiffrés ou sont chiffrés avec une clé KMS qui ne figure pas dans les paramètres fournis.

Identificateur : ENCRYPTED_VOLUMES

Types de ressources : AWS::EC2::Volume

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsId (facultatif), Type : chaîne

Identité ou ARN de la clé KMS utilisée pour chiffrer le volume.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

fms-shield-resource-policy-check

Vérifie si un Application Load Balancer, les CloudFront distributions Amazon, Elastic Load Balancer ou Elastic IP sont protégés par le Shield. AWS Il vérifie également s'ils ont une ACL Web associée aux distributions Application Load Balancer et Amazon CloudFront .

Identificateur : FMS_SHIELD_RESOURCE_POLICY_CHECK

Types de ressources : AWS::CloudFront::Distribution, AWS::ElasticLoad BalancingV2 : :LoadBalancer, AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoad Équilibrage : :, LoadBalancer AWS::ShieldRegional::Protection AWS::Shield::Protection

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

webACLId, Type : chaîne

WebACLId de la liste ACL web.

resourceTypes, Type : chaîne

La portée des ressources à laquelle cette règle de configuration sera appliquée.

resourceTags (facultatif), Type : chaîne

Les balises de ressource auxquelles la règle doit être associée (par exemple, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }).

excludeResourceTags (Facultatif), Type : valeur booléenne

Si la valeur est true, exclure les ressources qui correspondent à resourceTags. Si la valeur est false, inclure toutes les ressources qui correspondent à resourceTags.

fmsManagedToken (Facultatif), Type : chaîne

Un jeton généré par AWS Firewall Manager lors de la création de la règle dans votre compte. AWS Config ignore ce paramètre lorsque vous créez cette règle.

fmsRemediationEnabled (Facultatif), Type : valeur booléenne

Si cela est vrai, AWS Firewall Manager mettra à jour les ressources NON_COMPLIANT conformément à la politique du FMS. AWS Config ignore ce paramètre lorsque vous créez cette règle.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

fms-webacl-resource-policy-check

Vérifie si l'ACL Web est associée à un Application Load Balancer, à un stage API Gateway ou à des distributions Amazon CloudFront . Lors de la AWS Firewall Manager création de cette règle, le propriétaire de la politique FMS la spécifie `WebACLId` dans la stratégie FMS et peut éventuellement activer la correction.

Identificateur : FMS_WEBACL_RESOURCE_POLICY_CHECK

Types de ressources AWS::CloudFront::Distribution, AWS::ApiGateway : :Stage AWS::ElasticLoadBalancingV2::LoadBalancer, ACL AWS::WAFRegional::Web

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

webACLId, Type : chaîne

WebACLId de la liste ACL web.

resourceTags (facultatif), Type : chaîne

Les balises de ressources (ApplicationLoadéquilibreur ApiGatewayStage et CloudFront distributions) auxquelles la règle doit être associée. (par exemple, {« TagKey1" : [" tagValue1"], « tagKey2" : [" tagValue2", « tagValue3"]})

excludeResourceTags (Facultatif), Type : valeur booléenne

Si la valeur est true, les ressources qui correspondent à resourceTags sont exclues.

fmsManagedToken (Facultatif), Type : chaîne

Un jeton généré par AWS Firewall Manager lors de la création de la règle dans le compte client. AWS Config ignore ce paramètre lorsque le client crée cette règle.

fmsRemediationEnabled (Facultatif), Type : valeur booléenne

Si cela est vrai, AWS Firewall Manager mettra à jour les ressources non conformes conformément à la politique du FMS. AWS Config ignore ce paramètre lorsque le client crée cette règle.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

fms-webacl-rulegroup-association-check

Vérifie que les groupes de règles s'associent à la liste ACL Web à la bonne priorité. La bonne priorité est déterminée par le classement des groupes de règles dans le paramètre ruleGroups. Lors AWS Firewall Manager de la création de cette règle, elle attribue la priorité la plus élevée à 0, suivie de 1, 2, etc. Le propriétaire de la politique FMS spécifie le classement `ruleGroups` dans la politique FMS et peut éventuellement activer la correction.

Identificateur : FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Types de ressources : AWS::WAF::Web ACL, AWS::WAFRegional::Web ACL

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

ruleGroups, Type : chaîne

Liste de et paires séparées par des RuleGroupIds virgules. WafOverrideAction (par exemple, ruleGroupId -1:NONE, ruleGroupId 2:COUNT)

fmsManagedToken (Facultatif), Type : chaîne

Un jeton généré par AWS Firewall Manager lors de la création de la règle dans le compte client. AWS Config ignore ce paramètre lorsque le client crée cette règle.

fmsRemediationEnabled (Facultatif), Type : valeur booléenne

Si cela est vrai, AWS Firewall Manager mettra à jour les ressources non conformes conformément à la politique du FMS. AWS Config ignore ce paramètre lorsque le client crée cette règle.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

fsx-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour les systèmes de fichiers Amazon FSx. La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans le système de fichiers Amazon FSx.

Identificateur : FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::FSx::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des systèmes de fichiers Amazon FSx pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du système de fichiers Amazon FSx pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

fsx-lustre-copy-tags-to-backups

Vérifie si les systèmes de fichiers Amazon FSx pour Lustre sont configurés pour copier les balises dans les sauvegardes. La règle est NON_COMPLIANT si les systèmes de fichiers Lustre ne sont pas configurés pour copier les balises dans les sauvegardes.

Identificateur : FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

Types de ressources : AWS::FSx::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

fsx-meets-restore-time-target

Vérifie si la durée de restauration des systèmes de fichiers Amazon FSx est conforme à la durée spécifiée. La règle est NON_COMPLIANT si la durée LatestRestoreExecutionTimeMinutes d'un système de fichiers Amazon FSx est supérieure à quelques minutes. maxRestoreTime

Identifiant : FSX_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::FSx::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balises des systèmes de fichiers Amazon FSx pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

ID du système de fichiers Amazon FSx pour la règle à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

fsx-openzfs-copy-tags-enabled

Vérifie si les systèmes de fichiers Amazon FSx pour OpenZFS sont configurés pour copier les balises dans les sauvegardes et les volumes. La règle est NON_COMPLIANT si les systèmes de fichiers FSx pour OpenZFS ne sont pas configurés pour copier les balises vers les sauvegardes et les volumes.

Identificateur : FSX_OPENZFS_COPY_TAGS_ENABLED

Types de ressources : AWS::FSx::FileSystem

Type de déclencheur : périodique

Région AWS : uniquement disponible dans les régions Europe (Stockholm), Asie-Pacifique (Mumbai), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Asie-Pacifique (Hong Kong), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney) et Canada (Centre)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

fsx-resources-protected-by-backup-plan

Vérifie si les systèmes de fichiers Amazon FSx sont protégés par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué au système de fichiers Amazon FSx.

Identificateur : FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::FSx::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des systèmes de fichiers Amazon FSx pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du système de fichiers Amazon FSx pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

fsx-windows-audit-log-configured

Vérifie si l'audit d'accès aux fichiers est activé sur le système de fichiers Amazon FSx for Windows File Server. La règle est NON_COMPLIANT si l'audit d'accès aux fichiers n'est pas activé sur les systèmes de fichiers FSx for Windows File Server.

Identificateur : FSX_WINDOWS_AUDIT_LOG_CONFIGURED

Types de ressources : AWS::FSx::FileSystem

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

global-endpoint-event-replication-enabled

Vérifie si la réplication des événements est activée pour les points de terminaison EventBridge mondiaux Amazon. La règle est NON_COMPLIANT si la réplication d'événements n'est pas activé.

Identificateur : GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

Types de ressources : AWS::Events::Endpoint

Type de déclencheur : changements de configuration

Région AWS: Disponible uniquement en Europe (Stockholm), Asie-Pacifique (Mumbai), Europe (Paris), USA Est (Ohio), Europe (Irlande), Europe (Francfort), Amérique du Sud (Sao Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Séoul), Asie-Pacifique (Singapour), Asie-Pacifique (Asie-Pacifique), Asie-Pacifique (Asie-Pacifique) Sydney), Région du Canada (Centre)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

guardduty-eks-protection-audit activé

Vérifie si la surveillance du journal d'audit pour Amazon Elastic Kubernetes Service (Amazon EKS) est activée pour un détecteur GuardDuty Amazon sur votre compte. La règle est NON_COMPLIANT si la fonctionnalité de surveillance du journal d'audit EKS n'est pas activée pour votre compte.

Identifiant : GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

Types de ressources : AWS::GuardDuty::Detector

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

guardduty-eks-protection-runtime activé

Vérifie si Amazon EKS Runtime Monitoring avec gestion automatisée des agents est activé pour le GuardDuty détecteur dans votre compte. La règle est NON CONFORME si la surveillance du temps d'exécution EKS avec gestion automatique des agents n' GuardDuty est pas activée pour votre compte.

Identifiant : GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

Types de ressources : AWS::GuardDuty::Detector

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

guardduty-enabled-centralized

Vérifie si Amazon GuardDuty est activé dans votre AWS compte et dans votre AWS région. Si vous fournissez un AWS compte pour la centralisation, la règle évalue les GuardDuty résultats dans le compte centralisé. La règle est CONFORME lorsqu'elle GuardDuty est activée.

Identificateur : GUARDDUTY_ENABLED_CENTRALIZED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

CentralMonitoringAccount (Facultatif), Type : chaîne

> Liste de AWS comptes séparés par des virgules (12 chiffres) sur lesquels les GuardDuty résultats Amazon peuvent être centralisés.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

compatible avec la protection GuardDuty-Lambda

Vérifie si la protection Lambda est activée pour un GuardDuty détecteur Amazon dans votre compte. La règle est NON_COMPLIANT si la fonctionnalité de protection Lambda d'Amazon n' GuardDuty est pas activée pour votre compte.

Identifiant : GUARDDUTY_LAMBDA_PROTECTION_ENABLED

Types de ressources : AWS::GuardDuty::Detector

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

activé par guardduty-malware-protection

Vérifie si la protection contre les programmes malveillants est activée pour un GuardDuty détecteur Amazon sur votre compte. La règle est NON_COMPLIANT si la fonctionnalité de protection contre les programmes malveillants d'Amazon n' GuardDuty est pas activée pour votre compte.

Identifiant : GUARDDUTY_MALWARE_PROTECTION_ENABLED

Types de ressources : AWS::GuardDuty::Detector

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

guardduty-non-archived-findings

Vérifie si Amazon GuardDuty possède des résultats qui ne sont pas archivés. La règle est NON_COMPLIANT si GuardDuty des résultats de gravité faible/moyenne/élevée non archivés sont antérieurs au nombre spécifié dans le paramètre /days/. daysLowSev MediumSev `daysHighSev`

Identificateur : GUARDDUTY_NON_ARCHIVED_FINDINGS

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

daysLowSev (Facultatif), Type : int, Valeur par défaut : 30

Le nombre de jours pendant lesquels les résultats de GuardDuty faible gravité d'Amazon sont autorisés à ne pas être archivés. La durée par défaut est de 30 jours.

daysMediumSev (Facultatif), Type : int, Valeur par défaut : 7

Le nombre de jours pendant lesquels les résultats de gravité GuardDuty moyenne d'Amazon sont autorisés à ne pas être archivés. La durée par défaut est de 7 jours.

daysHighSev (Facultatif), Type : int, Valeur par défaut : 1

Le nombre de jours pendant lesquels les résultats GuardDuty les plus graves d'Amazon sont autorisés à ne pas être archivés. La valeur par défaut est de 1 jour.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

guardduty-rds-protection activé

Vérifie si la protection Amazon Relational Database Service (Amazon RDS) est activée pour un détecteur GuardDuty Amazon dans votre compte. La règle est NON_COMPLIANT si la fonctionnalité de protection Amazon RDS d'Amazon n' GuardDuty est pas activée pour votre compte.

Identifiant : GUARDDUTY_RDS_PROTECTION_ENABLED

Types de ressources : AWS::GuardDuty::Detector

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

protection guardduty-s3 activée

Vérifie si la protection S3 est activée pour un Amazon GuardDuty Detector sur votre compte. La règle est NON_COMPLIANT si la fonctionnalité de protection S3 d'Amazon n' GuardDuty est pas activée pour votre compte.

Identifiant : GUARDDUTY_S3_PROTECTION_ENABLED

Types de ressources : AWS::GuardDuty::Detector

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-customer-policy-blocked-kms-actions

Vérifie si les politiques gérées AWS d'Identity and Access Management (IAM) que vous créez n'autorisent pas les actions bloquées sur les clés KMS. AWS La règle est NON_COMPLIANT si une action bloquée est autorisée sur les clés AWS KMS par la politique IAM gérée.

> **Note**
>
> Cette règle n'évalue pas les variables ou les conditions dans les politiques IAM. Pour plus d'informations, voir Éléments de stratégie IAM : variables et éléments de stratégie IAM JSON : condition dans le guide de l'utilisateur IAM.

Identificateur : IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

Types de ressources : AWS::IAM::Policy

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

bloqué ActionsPatterns, Type : CSV

Liste séparée par des virgules de schémas d'action KMS bloqués. Par exemple, vous pouvez répertorier KMS:Decrypt* ou kms : comme modèles d'action bloqués. ReEncrypt La règle est NON_COMPLIANT si la politique IAM gérée autorise l'un des schémas d'action répertoriés dans ce paramètre.

exclure PermissionBoundaryPolicy (facultatif), Type : valeur booléenne

Indicateur booléen permettant d'exclure l'évaluation des politiques IAM utilisées comme limites d'autorisations. Si elle est définie sur « true », la règle n'inclura pas de limites d'autorisations dans l'évaluation. Sinon, toutes les politiques IAM concernées sont évaluées lorsque la valeur est définie sur « false ». La valeur par défaut est « false ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

compatible avec l'analyseur d'accès externe iam

Vérifie si un analyseur d'accès IAM pour l'accès externe est activé dans votre compte par région. La règle est NON_COMPLIANT s'il n'existe aucun analyseur d'accès externe dans la région ou si l'attribut « status » n'est pas défini sur « ACTIF ».

Identifiant : IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-group-has-users-check

Vérifie si les groupes IAM ont au moins un utilisateur IAM.

Identificateur : IAM_GROUP_HAS_USERS_CHECK

Types de ressources : AWS::IAM::Group

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-inline-policy-blocked-kms-actions

Vérifie si les politiques intégrées associées à vos utilisateurs, rôles et groupes IAM n'autorisent pas le blocage d'actions sur toutes les clés AWS KMS. La règle est NON_COMPLIANT si une action bloquée est autorisée sur toutes les clés AWS KMS dans une politique intégrée.

Identificateur : IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

Types de ressources : AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

bloqué ActionsPatterns, Type : CSV

Liste séparée par des virgules des modèles d'action KMS bloqués, par exemple, kms : *, KMS:Decrypt, kms : *. ReEncrypt

exclure RoleByManagementAccount (facultatif), Type : valeur booléenne

Un rôle doit être exclu s'il n'est assumé que par le compte de gestion de l'organisation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-no-inline-policy-check

Vérifie si la fonctionnalité de politique en ligne n'est pas utilisée. La règle est NON_COMPLIANT si un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) dispose d'une politique intégrée.

Identificateur : IAM_NO_INLINE_POLICY_CHECK

Types de ressources : AWS::IAM::User, AWS::IAM::Role, AWS::IAM::Group

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-password-policy

Vérifie si la politique de mot de passe du compte pour les utilisateurs d' AWS Identity and Access Management (IAM) répond aux exigences spécifiées dans les paramètres. La règle est

NON_COMPLIANT si la politique de mot de passe du compte ne répond pas aux exigences spécifiées.

> **Important**
>
> Les valeurs `true` et `false` des paramètres de règle sont sensibles à la casse. Si `true` n'est pas indiqué en minuscules, il sera traité comme `false`.

> **Note**
>
> Résultat de l'évaluation de la politique de mot de passe IAM par défaut
> Cette règle est marquée comme NON_COMPLIANT lorsque la politique de mot de passe IAM par défaut est utilisée.
> Règles gérées et types de ressources IAM globaux
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.
> Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.
> Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : IAM_PASSWORD_POLICY

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

RequireUppercaseCharacters (Facultatif), Type : valeur booléenne, Valeur par défaut : true

Au moins un caractère majuscule est requis dans le mot de passe.

RequireLowercaseCharacters (Facultatif), Type : valeur booléenne, Valeur par défaut : true

Au moins un caractère minuscule est requis dans le mot de passe.

RequireSymbols (Facultatif), Type : valeur booléenne, Valeur par défaut : true

Au moins un symbole est requis dans le mot de passe.

RequireNumbers (Facultatif), Type : valeur booléenne, Valeur par défaut : true

Au moins un chiffre est requis dans le mot de passe.

MinimumPasswordLength (Facultatif), Type : int, Valeur par défaut : 14

Longueur minimum du mot de passe.

PasswordReusePrevention (Facultatif), Type : int, Valeur par défaut : 24

Nombre de mots de passe avant d'autoriser la réutilisation.

MaxPasswordAge (Facultatif), Type : int, Valeur par défaut : 90

Nombre de jours avant l'expiration du mot de passe.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

iam-policy-blacklisted-check

Vérifie dans chaque ressource AWS Identity and Access Management (IAM) si une politique Amazon Resource Name (ARN) dans le paramètre d'entrée est attachée à la ressource IAM. La règle est NON_COMPLIANT si l'ARN de politique est associé à la ressource IAM.

Identificateur : IAM_POLICY_BLACKLISTED_CHECK

Types de ressources : AWS::IAM::User, AWS::IAM::Group, AWS::IAM::Role

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

policyArns, Type : CSV, Par défaut : arn:aws:iam : :aws:policy/ AdministratorAccess

Liste d'ARN de politique IAM séparés par des virgules qui ne doivent être associés à aucune entité IAM.

exceptionList (facultatif), Type : CSV

Liste des types de ressources séparés par des virgules et liste des paires de noms de ressources. Par exemple, users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3].

> **Note**
>
> Pour la liste des exceptions, spécifiez le nom de la ressource et non l'ARN complet. Non valide :`arn:aws:iam::444455556666:role/Admin`. Valide :`Admin`.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-policy-in-use

Vérifie si l'ARN de politique IAM est associé à un utilisateur IAM, à un groupe comprenant un ou plusieurs utilisateurs IAM ou à un rôle IAM présentant une ou plusieurs entités approuvées.

> **Note**
>
> Règles gérées et types de ressources IAM globaux
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.
> Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : IAM_POLICY_IN_USE

Types de ressources : AWS::IAM::Policy

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

policyARN, Type : chaîne

ARN de politique IAM devant être vérifié.

policyUsageType (Facultatif), Type : chaîne

Spécifiez la politique à associée à un utilisateur, groupe ou rôle IAM. Les valeurs valides sont IAM_USER, IAM_GROUP, IAM_ROLE ou ANY. La valeur par défaut est ANY.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-policy-no-statements-with-admin-access

Vérifie si les politiques AWS Identity and Access Management (IAM) que vous créez comportent des instructions Allow qui accordent des autorisations pour toutes les actions sur toutes les ressources. La règle est NON_COMPLIANT si une instruction de la politique IAM gérée par le client inclut « Effect » : « Allow » avec « Action » : « * » sur « Resource » : « * ».

> **Note**
>
> Cette règle évalue uniquement les politiques gérées par le client. Cette règle n'évalue PAS les politiques intégrées ou les politiques AWS gérées. Pour plus d'informations sur les

différences, consultez Politiques gérées et politiques en ligne dans le Guide de l'utilisateur IAM.

La politique suivante est NON_COMPLIANT :

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

La politique suivante est COMPLIANT :

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

Identificateur : IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

Types de ressources : AWS::IAM::Policy

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

exclure PermissionBoundaryPolicy (facultatif), Type : valeur booléenne

Indicateur booléen permettant d'exclure l'évaluation des politiques IAM utilisées comme limites d'autorisations. Si elle est définie sur « true », la règle n'inclura pas de limites d'autorisations dans l'évaluation. Sinon, toutes les politiques IAM concernées sont évaluées lorsque la valeur est définie sur « false ». La valeur par défaut est « false ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-policy-no-statements-with-full-access

Vérifie si les politiques AWS Identity and Access Management (IAM) que vous créez accordent des autorisations à toutes les actions sur des ressources individuelles. AWS La règle est NON_COMPLIANT si une politique IAM gérée par le client autorise un accès complet à au moins un service. AWS

Contexte : conformément au principe du moindre privilège, il est recommandé de limiter les actions autorisées dans vos politiques IAM lorsque vous accordez des autorisations aux AWS services. Cette approche permet de garantir que vous n'accordez que les autorisations nécessaires en spécifiant les actions exactes requises, évitant ainsi l'utilisation de caractères génériques illimités pour un service, tel que. `ec2:*`

Dans certains cas, vous souhaiterez peut-être autoriser plusieurs actions avec un préfixe similaire, par exemple DescribeFlowLogs et DescribeAvailabilityZones. Dans ces cas, vous pouvez ajouter un caractère générique suffixé au préfixe commun (par exemple,). `ec2:Describe*` Le regroupement d'actions associées peut aider à éviter d'atteindre les limites de taille fixées par la politique IAM.

Cette règle renverra COMPLIANT si vous utilisez des actions préfixées avec un caractère générique suffixé (par exemple,). `ec2:Describe*` Cette règle ne renverra NON_COMPLIANT que si vous utilisez des caractères génériques non restreints (par exemple,). `ec2:*`

> **Note**
>
> Cette règle évalue uniquement les politiques gérées par le client. Cette règle n'évalue PAS les politiques intégrées ou les politiques AWS gérées. Pour plus d'informations sur les différences, consultez Politiques gérées et politiques en ligne dans le Guide de l'utilisateur IAM.

Identificateur : IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Types de ressources : AWS::IAM::Policy

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

exclure PermissionBoundaryPolicy (facultatif), Type : valeur booléenne

Indicateur booléen permettant d'exclure l'évaluation des politiques IAM utilisées comme limites d'autorisations. Si elle est définie sur « true », la règle n'inclura pas de limites d'autorisations dans l'évaluation. Sinon, toutes les politiques IAM concernées sont évaluées lorsque la valeur est définie sur « false ». La valeur par défaut est « false ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-role-managed-policy-check

Vérifie si toutes les politiques gérées spécifiées dans la liste des politiques gérées sont associées au rôle AWS Identity and Access Management (IAM). La règle est NON_COMPLIANT si le rôle IAM n’est pas associé à une politique gérée.

Identificateur : IAM_ROLE_MANAGED_POLICY_CHECK

Types de ressources : AWS::IAM::Role

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

géré PolicyArns, Type : CSV

Liste séparée par des virgules des AWS politiques gérées Amazon Resource Names (ARN). Pour plus d'informations, consultez Amazon Resource Names (ARN) et Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-root-access-key-check

Vérifie si la clé d'accès d'utilisateur root est disponible. La règle est COMPLIANT si la clé d'accès d'utilisateur n'existe pas. Dans le cas contraire, la règle est NON_COMPLIANT.

> **Note**
>
> Règles gérées et types de ressources IAM globaux
>
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.
>
> Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.
>
> Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : IAM_ROOT_ACCESS_KEY_CHECK

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

vérification de l'expiration du certificat du serveur iam

Vérifie si les certificats de serveur AWS IAM SSL/TLS stockés dans IAM ont expiré. La règle est NON_COMPLIANT si un certificat de serveur IAM a expiré.

Identifiant : IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

Types de ressources : AWS::IAM::ServerCertificate

Type de déclencheur : périodique

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

iam-user-group-membership-check

Vérifie si les utilisateurs IAM appartiennent à au moins un groupe IAM.

Identificateur : IAM_USER_GROUP_MEMBERSHIP_CHECK

Types de ressources : AWS::IAM::User

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

groupNames (facultatif), Type : chaîne

Liste de groupes IAM séparés par des virgules auxquels les utilisateurs IAM doivent appartenir.

> **Note**
>
> Cette règle ne prend pas en charge les noms de groupe avec des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-user-mfa-enabled

Vérifie si l'authentification multifactorielle (MFA) est activée pour les utilisateurs d' AWS Identity and Access Management (IAM). La règle est NON_COMPLIANT si la MFA n'est pas activée pour au moins un utilisateur IAM.

> **Note**
>
> Règles gérées et types de ressources IAM globaux
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`AWS::IAM::Role, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.
> Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.
> Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : IAM_USER_MFA_ENABLED

Types de ressources : AWS::IAM::User

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-user-no-policies-check

Vérifie si aucun de vos utilisateurs AWS d'Identity and Access Management (IAM) n'est associé à des politiques. Les utilisateurs IAM doivent hériter des autorisations de groupes ou rôles IAM. La règle est NON_COMPLIANT si au moins un utilisateur IAM est associé à des politiques.

Identificateur : IAM_USER_NO_POLICIES_CHECK

Types de ressources : AWS::IAM::User

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

iam-user-unused-credentials-check

Vérifie si vos utilisateurs AWS Identity and Access Management (IAM) ont des mots de passe ou des clés d'accès actives qui n'ont pas été utilisés pendant le nombre de jours que vous avez indiqué. La règle est NON_COMPLIANT si des comptes inactifs n'ont pas été utilisés récemment.

> **Note**
>
> Calendrier de réévaluation

Réévaluer cette règle dans un délai de 4 heures après la première évaluation n'aura aucun effet sur les résultats.

Règles gérées et types de ressources IAM globaux

Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : IAM_USER_UNUSED_CREDENTIALS_CHECK

Types de ressources : AWS::IAM::User

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

CredentialUsageâge maximum, Type : int, Valeur par défaut : 90

Nombre maximal de jours pendant lesquels des informations d'identification ne peuvent pas être utilisées. La valeur par défaut est 90 jours.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

restricted-ssh

> **Important**
>
> L'identificateur (INCOMING_SSH_DISABLED) et le nom de cette règle (restricted-ssh) sont différents.

Vérifie que le trafic SSH entrant pour les groupes de sécurité est accessible. La règle est COMPLIANT si les adresses IP du trafic SSH entrant dans les groupes de sécurité sont limitées (CIDR autre que 0.0.0.0/0 ou ::/0). Dans le cas contraire, la règle est NON_COMPLIANT.

Identificateur : INCOMING_SSH_DISABLED

Types de ressources : AWS::EC2::SecurityGroup

Type de déclencheur : modifications de configuration et périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

compatible avec inspector-ec2-scan

Vérifie si le scan Amazon Inspector V2 EC2 est activé pour votre environnement à compte unique ou multicompte afin de détecter les vulnérabilités potentielles et les problèmes d'accessibilité réseau sur vos instances EC2. La règle est NON_COMPLIANT si le scan EC2 n'est pas activé.

Identifiant : INSPECTOR_EC2_SCAN_ENABLED

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

compatible avec inspector-ecr-scan

Vérifie si le scan ECR Amazon Inspector V2 est activé pour votre environnement à compte unique ou multicompte afin de détecter les vulnérabilités logicielles potentielles dans vos images de conteneur. La règle est NON_COMPLIANT si le scan ECR n'est pas activé.

Identifiant : INSPECTOR_ECR_SCAN_ENABLED

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

compatible avec le scan de code inspector-lambda

Vérifie si le scan du code Lambda Amazon Inspector V2 est activé pour votre environnement à compte unique ou multicompte afin de détecter les vulnérabilités potentielles du code. La règle est NON_COMPLIANT si le scan du code Lambda n'est pas activé.

Identifiant : INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Disponible uniquement en Europe (Stockholm), USA Est (Ohio), Europe (Irlande), Europe (Francfort), USA Est (Virginie du Nord), Europe (Londres), Asie-Pacifique (Tokyo), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

inspector-lambda compatible avec le scan standard

Vérifie si le scan standard Amazon Inspector V2 Lambda est activé pour votre environnement à compte unique ou multicompte afin de détecter les vulnérabilités logicielles potentielles. La règle est NON_COMPLIANT si le scan standard Lambda n'est pas activé.

Identifiant : INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ec2-instances-in-vpc

> **Important**
>
> L'identificateur (INSTANCES_IN_VPC) et le nom (ec2-instances-in-vpc) de cette règle sont différents.

Vérifie que vos instances EC2 appartiennent à un réseau cloud privé virtuel (VPC). Vous pouvez aussi spécifier l'ID du VPC à associer à vos instances.

Identificateur : INSTANCES_IN_VPC

Types de ressources : AWS::EC2::Instance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

vpcId (facultatif), Type : chaîne

ID du réseau VPC qui contient ces instances EC2.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

internet-gateway-authorized-vpc-only

Vérifie si les passerelles Internet sont associées à un réseau cloud virtuel privé autorisé (Amazon VPC). La règle est NON_COMPLIANT si des passerelles Internet sont associées à un réseau VPC non autorisé.

Identificateur : INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

Types de ressources : AWS::EC2::InternetGateway

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

AuthorizedVpcIds (Facultatif), Type : chaîne

Liste des ID de réseaux VPC autorisés séparés par des virgules avec passerelles Internet attachées. Si le paramètre n'est pas fourni, tous les passerelles Internet attachées seront NON_COMPLIANT.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

Kinesis-Firehose Delivery-Stream crypté

Vérifie si les flux de diffusion Amazon Kinesis Data Firehose sont chiffrés au repos avec un chiffrement côté serveur. La règle est NON_COMPLIANT si un flux de diffusion Kinesis Data Firehose n'est pas chiffré au repos par chiffrement côté serveur.

Identifiant : KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

Types de ressources : AWS::KinesisFirehose::DeliveryStream

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

Liste séparée par des virgules des Key Arns KMS approuvés pour l'utilisation de Kinesis Firehose.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

kinesis-stream-encrypted

Vérifie si les flux Amazon Kinesis sont chiffrés au repos avec le chiffrement côté serveur. La règle est NON_COMPLIANT pour un flux Kinesis si « StreamEncryption » n'est pas présent.

Contexte : Le chiffrement côté serveur est une fonctionnalité d'Amazon Kinesis Data Streams qui chiffre automatiquement les données avant qu'elles ne soient inactives à l'aide d'une clé KMS. AWS Les données sont chiffrées avant leur écriture sur la couche de stockage du flux Kinesis et déchiffrées après leur extraction de l'espace de stockage. Par conséquent, vos données sont chiffrées au repos dans le service Kinesis Data Streams. Vous pouvez ainsi respecter des exigences réglementaires strictes et améliorer la sécurité de vos données. Pour plus d'informations, consultez Protection des données dans Amazon Kinesis Data Streams.

Identificateur : KINESIS_STREAM_ENCRYPTED

Types de ressources : AWS::Kinesis::Stream

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

kms-cmk-not-scheduled-for-deletion

Vérifie si la suppression des AWS clés du service de gestion des clés (AWS KMS) n'est pas planifiée dans AWS KMS. La règle est NON_COMPLIANT si la suppression des clés KMS est planifiée.

Identificateur : KMS_CMK_NOT_SCHEDULED_FOR_DELETION

Types de ressources : AWS::KMS::Key

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyIds (Facultatif), Type : chaîne

Liste des ID de clé spécifiques gérées par les clients à ne pas planifier pour la suppression, séparés par des virgules. Si vous ne spécifiez aucune clé, la règle vérifie toutes les clés.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

lambda-concurrency-check

Vérifie si la fonction Lambda est configurée avec une limite d'exécution simultanée au niveau de la fonction. La règle est NON_COMPLIANT si la fonction Lambda n'est pas configurée avec la limite d'exécution simultanée au niveau de la fonction.

Identificateur : LAMBDA_CONCURRENCY_CHECK

Types de ressources : AWS::Lambda::Function

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

ConcurrencyLimitLow (Facultatif), Type : chaîne

Limite minimale d'exécution de simultanéité

ConcurrencyLimitHigh (Facultatif), Type : chaîne

Limite maximale d'exécution de simultanéité

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

lambda-dlq-check

Vérifie si une fonction Lambda est configurée avec une file d'attente de lettres mortes. La règle est NON_COMPLIANT si la fonction Lambda n'est pas configurée avec une file d'attente de lettres mortes.

Identificateur : LAMBDA_DLQ_CHECK

Types de ressources : AWS::Lambda::Function

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

dlqArns (facultatif), Type : chaîne

> Liste d'ARN Amazon SQS et Amazon SNS séparés par des virgules, qui doivent être configurés en tant que cible de la file d'attente de lettres mortes de la fonction Lambda.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

lambda-function-public-access-prohibited

Vérifie si la politique AWS Lambda fonctionnelle attachée à la ressource Lambda interdit l'accès public. Si la politique de la fonction Lambda autorise l'accès public, la règle est NON_COMPLIANT.

Contexte : Une politique de fonction lambda est considérée comme autorisant l'accès public si l'élément principal est vide ou contient un caractère générique. Par exemple, si l'élément principal est `“”` ou`{“AWS”: “”}`. Pour des raisons de sécurité, il n'est pas recommandé d'accorder un accès public. Restreindre l'accès public peut vous aider à empêcher les invocations non autorisées de vos fonctions Lambda, qui pourraient compromettre vos données ou entraîner des coûts indésirables.

Pour restreindre l'accès à vos fonctions Lambda, spécifiez les identifiants de AWS compte ou les Amazon Resource Names (ARN) des utilisateurs, rôles ou services IAM qui peuvent appeler les fonctions. Pour plus d'informations, consultez la section [Accorder l'accès aux fonctions à d'autres comptes] dans le Guide du AWS Lambda développeur.

Identificateur : LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

Types de ressources : AWS::Lambda::Function

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

lambda-function-settings-check

Vérifie si les paramètres de la fonction AWS Lambda relatifs à l'exécution, au rôle, au délai d'expiration et à la taille de la mémoire correspondent aux valeurs attendues. La règle ignore les fonctions dont le type de package est « Image » et les fonctions dont l'exécution est définie sur « Exécution uniquement pour le système d'exploitation ». La règle est NON_COMPLIANT si les paramètres de la fonction Lambda ne correspondent pas aux valeurs attendues.

Identificateur : LAMBDA_FUNCTION_SETTINGS_CHECK

Types de ressources : AWS::Lambda::Function

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

runtime, Type : CSV

Liste des valeurs d'exécution Lambda AWS séparées par des virgules

role (facultatif), Type : chaîne

Nom ou ARN du rôle d' AWS exécution Lambda

timeout (facultatif), Type : int, Valeur par défaut : 3

AWS Délai d'expiration de la fonction Lambda en secondes

memorySize (facultatif), Type : int, Valeur par défaut : 128

AWS Taille de la fonction Lambda en mégaoctets

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* Pour plus d'informations sur les valeurs valides pour ces entrées, voir Rôle MemorySize, temps d'exécution et délai d'expiration dans le guide de l' AWS CloudFormation utilisateur.

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

lambda-inside-vpc

Vérifie si une fonction Lambda est autorisée à accéder à un réseau cloud privé virtuel (VPC). La règle est NON_COMPLIANT si la Fonction Lambda ne se trouve pas dans un réseau VPC.

Identificateur : LAMBDA_INSIDE_VPC

Types de ressources : AWS::Lambda::Function

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

subnetIds (facultatif), Type : chaîne

Liste des ID de sous-réseau séparés par des virgules auxquels les fonctions Lambda peuvent être associées.

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

lambda-vpc-multi-az-check

Vérifie si Lambda est associé à plus d'une zone de disponibilité. La règle est NON_COMPLIANT si une seule zone de disponibilité est associée au Lambda ou si le nombre de zones de disponibilité associées est inférieur au nombre indiqué dans le paramètre facultatif.

Identificateur : LAMBDA_VPC_MULTI_AZ_CHECK

Types de ressources : AWS::Lambda::Function

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

availabilityZones (facultatif), Type : int

Nombre de zones de disponibilité attendues.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

vérification automatique de la découverte des données Macie-Auto-Sensitive

Vérifie si la découverte automatique des données sensibles est activée pour Amazon Macie. La règle est NON_COMPLIANT si la découverte automatique des données sensibles est désactivée. La règle est APPLICABLE pour les comptes administrateurs et NOT_APPLICABLE pour les comptes membres.

Identifiant : MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

macie-status-check

Vérifie si Amazon Macie est activé dans votre compte par région. La règle est NON_COMPLIANT si l'attribut « status » n'est pas défini sur « ENABLED ».

Identificateur : MACIE_STATUS_CHECK

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

mfa-enabled-for-iam-console-access

Vérifie si l' AWS authentification multifactorielle (MFA) est activée pour AWS tous les utilisateurs d'Identity and Access Management (IAM) qui utilisent un mot de passe de console. La règle est COMPLIANT lorsque MFA est activé.

> **Note**
>
> Calendrier de réévaluation
> Réévaluer cette règle dans un délai de 4 heures après la première évaluation n'aura aucun effet sur les résultats.
> Règles gérées et types de ressources IAM globaux
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`AWS::IAM::Role, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.
Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

Types de ressources : AWS::IAM::User

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

mq-active-deployment-mode

Vérifie le mode de déploiement configuré pour le moteur d'agent Amazon MQ ActiveMQ. La règle est NON_COMPLIANT si le mode d'agent à instance unique par défaut est utilisé.

Identificateur : MQ_ACTIVE_DEPLOYMENT_MODE

Types de ressources : AWS::AmazonMQ::Broker

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

mq-automatic-minor-version-upgrade-enabled

Vérifie si les mises à niveau automatiques de versions mineures sont activées pour les agents Amazon MQ. La règle est NON_COMPLIANT si le champ « AutoMinor VersionUpgrade » n'est pas activé pour un courtier Amazon MQ.

Identificateur : MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Types de ressources : AWS::AmazonMQ::Broker

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

mq-auto-minor-version-upgrade-enabled

Vérifie si les mises à niveau automatiques de versions mineures sont activées pour les agents Amazon MQ. La règle est NON_COMPLIANT si le champ « AutoMinor VersionUpgrade » n'est pas activé pour un courtier Amazon MQ.

Identificateur : MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

Types de ressources : AWS::AmazonMQ::Broker

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

mq-cloudwatch-audit-logging-enabled

Vérifie si les courtiers Amazon MQ ont activé la journalisation des CloudWatch audits Amazon. La règle est NON_COMPLIANT si la journalisation des audits n'est pas activée sur un agent.

Identificateur : MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

Types de ressources : AWS::AmazonMQ::Broker

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

compatible avec mq-cloudwatch-audit-log

Vérifie si la journalisation des CloudWatch audits est activée pour un courtier Amazon MQ. La règle est NON_COMPLIANT si la journalisation des audits n'est pas activée sur le broker.

Identifiant : MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

Types de ressources : AWS::AmazonMQ::Broker

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

mq-no-public-access

Vérifie si les agents Amazon MQ ne sont pas accessibles publiquement. La règle est NON_COMPLIANT si le champ « PubliclyAccessible » est défini sur true pour un courtier Amazon MQ.

Identificateur : MQ_NO_PUBLIC_ACCESS

Types de ressources : AWS::AmazonMQ::Broker

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

mq-rabbit-deployment-mode

Vérifie le mode de déploiement configuré pour le moteur d'agent Amazon MQ RabbitMQ. La règle est NON_COMPLIANT si le mode d'agent à instance unique par défaut est utilisé.

Identificateur : MQ_RABBIT_DEPLOYMENT_MODE

Types de ressources : AWS::AmazonMQ::Broker

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

msk-enhanced-monitoring-enabled

Vérifie si la surveillance améliorée est activée pour un cluster Amazon MSK défini sur PER_TOPIC_PER_BROKER ou PER_TOPIC_PER_PARTITION. La règle est NON_COMPLIANT si la surveillance améliorée est activée et définie sur DEFAULT ou PER_BROKER.

Identificateur : MSK_ENHANCED_MONITORING_ENABLED

Types de ressources : AWS::MSK::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

msk-in-cluster-node-require-tls

Vérifie si un cluster Amazon MSK applique le chiffrement en transit à l'aide du protocole HTTPS (TLS) avec les nœuds d'agent du cluster. La règle est NON_COMPLIANT si la communication en texte brut est activée pour les connexions de nœuds d'agent au sein du cluster.

Identifiant : MSK_IN_CLUSTER_NODE_REQUIRE_TLS

Types de ressources : AWS::MSK::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

multi-region-cloudtrail-enabled

> **Important**
>
> L'identificateur (MULTI_REGION_CLOUD_TRAIL_ENABLED) et le nom (multi-region-cloudtrail-enabled) de cette règle sont différents.

Vérifie s'il existe au moins une région multiple. AWS CloudTrail La règle est NON_COMPLIANT si les journaux de suivi ne correspondent pas aux paramètres d'entrée. La règle est NON_COMPLIANT si le `ExcludeManagementEventSources` champ n'est pas vide ou s'il AWS CloudTrail est configuré pour exclure des événements de gestion tels que des événements ou AWS KMS des événements d'API Amazon RDS Data.

Identificateur : MULTI_REGION_CLOUD_TRAIL_ENABLED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

s3 BucketName (facultatif), Type : chaîne

Nom du compartiment Amazon S3 AWS CloudTrail auquel les fichiers journaux doivent être envoyés.

snsTopicArn (Facultatif), Type : chaîne

ARN de rubrique Amazon SNS AWS CloudTrail à utiliser pour les notifications.

cloud WatchLogsLogGroupArn (facultatif), Type : chaîne

ARN du groupe de CloudWatch journaux Amazon AWS CloudTrail auquel envoyer des données.

includeManagementEvents (Facultatif), Type : valeur booléenne

Sélecteur d'événements pour inclure les événements de gestion pour. AWS CloudTrail

readWriteType (Facultatif), Type : chaîne

Type d'événements à enregistrer. Les valeurs valides sont ReadOnly, WriteOnly et ALL.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

nacl-no-unrestricted-ssh-rdp

Vérifie si les ports par défaut du trafic entrant SSH/RDP pour les listes de contrôle d'accès réseau (NACL) ne sont pas restreints. La règle est NON_COMPLIANT si une entrée NACL entrante autorise un bloc d'adresse source CIDR TCP ou UDP pour les ports 22 ou 3389.

Identificateur : NACL_NO_UNRESTRICTED_SSH_RDP

Types de ressources : AWS::EC2::NetworkAcl

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-backup-retention-check

Vérifie si la période de conservation d'un cluster de bases de données Amazon Neptune est définie sur un nombre de jours spécifique. La règle est NON_COMPLIANT si la période de conservation est inférieure à la valeur spécifiée par le paramètre.

Identificateur : NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

minimum BackupRetentionPeriod (facultatif), Type : int

> Les sauvegardes doivent être conservées pendant un nombre minimal de jours. Les valeurs valides sont comprises entre 1 et 35, la valeur par défaut est 7. La règle est NON_COMPLIANT si la valeur est supérieure à « sauvegarde »RetentionPeriod. La règle est CONFORME si la valeur est inférieure ou égale à « sauvegarde RetentionPeriod ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

neptune-cluster-cloudwatch-log-export-enabled

Vérifie si l'exportation des journaux est activée pour les CloudWatch journaux d'audit d'un cluster Amazon Neptune. La règle est NON_COMPLIANT si l'exportation des journaux n'est pas activée pour les CloudWatch journaux d'audit d'un cluster Neptune.

Identificateur : NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-copy-tags-to-snapshot-enabled

Vérifie si un cluster Amazon Neptune est configuré pour copier toutes les balises dans les instantanés lorsque ceux-ci sont créés. La règle est NON_COMPLIANT si « copy TagsTo Snapshot » est défini sur false.

Identificateur : NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-deletion-protection-enabled

Vérifie si la protection contre la suppression est activée pour un cluster de base de données Amazon Neptune. La règle est NON_COMPLIANT si le champ deletionProtection d'un cluster Amazon Neptune est défini sur false.

Identificateur : NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-encrypted

Vérifie si le chiffrement du stockage est activé pour vos clusters de base de données Amazon Neptune. La règle est NON_COMPLIANT si le chiffrement du stockage n'est pas activé.

Identificateur : NEPTUNE_CLUSTER_ENCRYPTED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

KmsKeyArns (Facultatif), Type : CSV

> Une liste séparée par des virgules des ARN des clés KMS à comparer avec celle KmsKeyId du cluster chiffré.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-iam-database-authentication

Vérifie si l'authentification de base de données AWS Identity and Access Management (IAM) est activée sur un cluster Amazon Neptune. La règle est NON_COMPLIANT si l'authentification de base de données IAM n'est pas activée sur un cluster Amazon Neptune.

Identificateur : NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-multi-az-enabled

Vérifie si un cluster Amazon Neptune est configuré avec la réplication Amazon RDS Multi-AZ. La règle est NON_COMPLIANT si la réplication Multi-AZ n'est pas activée.

Identificateur : NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-snapshot-encrypted

Vérifie si les instantanés sont chiffrés dans un cluster de bases de données Amazon Neptune. La règle est NON_COMPLIANT si les instantanés d'un cluster Neptune ne sont pas chiffrés.

Identificateur : NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

Types de ressources : AWS : :RDS : :DB ClusterSnapshot

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

neptune-cluster-snapshot-public-prohibited

Vérifie si un instantané de cluster de base de données manuel Amazon Neptune est public. La règle est NON_COMPLIANT si des instantanés de cluster Neptune nouveaux ou existants sont publics.

Identificateur : NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Types de ressources : AWS : :RDS : :DB ClusterSnapshot

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

netfw-deletion-protection-enabled

Vérifie si la protection contre les suppressions est activée sur AWS Network Firewall. La règle est NON_COMPLIANT si la protection contre la suppression n'est pas activée pour Network Firewall.

Identificateur : NETFW_DELETION_PROTECTION_ENABLED

Types de ressources : AWS::NetworkFirewall::Firewall

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

netfw-logging-enabled

Vérifie si la journalisation est activée sur les pare-feux AWS Network Firewall. Cette règle est NON_COMPLIANT si un type de journalisation spécifique n'est pas configuré. Vous pouvez spécifier le type de journalisation que vous souhaitez vérifier à l'aide de cette règle.

Identificateur : NETFW_LOGGING_ENABLED

Types de ressources : AWS::NetworkFirewall::LoggingConfiguration

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

logType (facultatif), Type : chaîne

logType (facultatif) : type de journal devant être vérifié dans les pare-feux à l'aide de la règle : « alert », « flow » ou « both ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

netfw-multi-az-enabled

Vérifie si les pare-feux AWS Network Firewall sont déployés dans plusieurs zones de disponibilité. La règle est NON_COMPLIANT si les pare-feux sont déployés dans une seule zone de disponibilité ou dans un nombre de zones inférieur au nombre indiqué dans le paramètre facultatif.

Identificateur : NETFW_MULTI_AZ_ENABLED

Types de ressources : AWS::NetworkFirewall::Firewall

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

availabilityZones (facultatif), Type : int

Nombre de zones de disponibilité attendues.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

netfw-policy-default-action-fragment-packets

Vérifie si une politique AWS Network Firewall est configurée avec une action par défaut sans état définie par l'utilisateur pour les paquets fragmentés. La règle est NON_COMPLIANT si l'action par défaut sans état pour les paquets fragmentés ne correspond pas à l'action par défaut définie par l'utilisateur.

Identificateur : NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

Types de ressources : AWS::NetworkFirewall::FirewallPolicy

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Actions FragmentDefault apatrides, Type : CSV

Liste de valeurs séparées par des virgules. Vous pouvez en sélectionner deux au maximum. Les valeurs valides sont « aws:pass », « aws:drop » et « aws:forward_to_sfe ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

netfw-policy-default-action-full-packets

Vérifie si une politique AWS Network Firewall est configurée avec une action apatride par défaut définie par l'utilisateur pour les paquets complets. La règle est NON_COMPLIANT si l'action par défaut sans état pour les paquets complets ne correspond pas à l'action par défaut sans état définie par l'utilisateur.

Identificateur : NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

Types de ressources : AWS::NetworkFirewall::FirewallPolicy

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

apatride DefaultActions, Type : CSV

Liste de valeurs séparées par des virgules. Vous pouvez en sélectionner deux au maximum. Les valeurs valides sont « aws:pass », « aws:drop » et « aws:forward_to_sfe ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

netfw-policy-rule-group-associated

Vérifiez que la politique de AWS Network Firewall est associée à des groupes de règles dynamiques OU apatrides. Cette règle est NON_COMPLIANT si aucun groupe avec ou sans état n'est associé à la politique Network Firewall. Elle est COMPLIANT si l'un des groupes de règles existe.

Identificateur : NETFW_POLICY_RULE_GROUP_ASSOCIATED

Types de ressources : AWS::NetworkFirewall::FirewallPolicy

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

netfw-stateless-rule-group-not-empty

Vérifie si un groupe de règles Network Firewall sans état contient des règles. La règle est NON_COMPLIANT si aucune règle ne figure dans un groupe de règles Network Firewall sans état.

Identificateur : NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Types de ressources : AWS::NetworkFirewall::RuleGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

nlb-cross-zone-load-balancing-enabled

Vérifie si l'équilibrage de charge entre zones est activé sur les Network Load Balancers (NLB). La règle est NON_COMPLIANT si l'équilibrage de charge entre zones n'est pas activé sur un NLB.

Identificateur : NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Types de ressources : AWS::ElasticLoadBalancingV2::LoadBalancer

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

no-unrestricted-route-to-igw

Vérifie s'il existe des routes publiques vers une passerelle Internet (IGW) dans la table de routage. La règle est NON_COMPLIANT si une route vers une IGW présente un bloc d'adresses CIDR de destination « 0.0.0.0/0 » ou « ::/0 » ou si un bloc d'adresses CIDR de destination ne correspond pas au paramètre de règle.

Identificateur : NO_UNRESTRICTED_ROUTE_TO_IGW

Types de ressources : AWS::EC2::RouteTable

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

routeTableIds (Facultatif), Type : CSV

Liste des ID de table de routage séparés par des virgules, susceptibles de présenter des routes vers une passerelle Internet avec un bloc d'adresses CIDR de destination « 0.0.0.0/0 » ou « ::/0 ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

opensearch-access-control-enabled

Vérifie si le contrôle d'accès détaillé est activé dans les domaines Amazon OpenSearch Service. La règle est NON_COMPLIANT si elle n' AdvancedSecurityOptions est pas activée pour le domaine de OpenSearch service.

Identificateur : OPENSEARCH_ACCESS_CONTROL_ENABLED

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

opensearch-audit-logging-enabled

Vérifie si la journalisation des audits est activée dans les domaines Amazon OpenSearch Service. La règle est NON_COMPLIANT si la journalisation des audits n'est pas activée dans un domaine de OpenSearch service.

Identificateur : OPENSEARCH_AUDIT_LOGGING_ENABLED

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

cloud WatchLogsLogGroupArnList (facultatif), Type : CSV

Liste séparée par des virgules des noms de ressources Amazon (ARN) pour les groupes de CloudWatch journaux Amazon Logs. La règle vérifie si les groupes de journaux spécifiés sont configurés pour les journaux d'audit.

Les valeurs valides sont : `arn:aws:logs:region:account-id:log-group:log_group_name:*` et `arn:aws:logs:region:account-id:log-group:log_group_name`.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

opensearch-data-node-fault-tolerance

Vérifie si les domaines Amazon OpenSearch Service sont configurés avec au moins trois nœuds de données et si zoneAwarenessEnabled c'est vrai. La règle est NON_COMPLIANT pour un OpenSearch domaine si « InstanceCount » est inférieur à 3 ou si « zone » est défini sur « false ». AwarenessEnabled

Identificateur : OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

opensearch-encrypted-at-rest

Vérifie si la configuration du chiffrement au repos est activée pour les domaines Amazon OpenSearch Service. La règle est NON_COMPLIANT si le champ `EncryptionAtRestOptions` n'est pas activé.

> **Note**
>
> La règle n'évalue pas les domaines Elasticsearch.

Identificateur : OPENSEARCH_ENCRYPTED_AT_REST

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

opensearch-https-required

Vérifie si les connexions aux OpenSearch domaines utilisent le protocole HTTPS. La règle est NON_COMPLIANT si le OpenSearch domaine Amazon « EnforceHTTPS » n'est pas « vrai » ou est « vrai » et que « TLS » n'est pas dans « SecurityPolicy ». `tlsPolicies`

Identificateur : OPENSEARCH_HTTPS_REQUIRED

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

tlsPolicies (facultatif), Type : CSV

Liste séparée par des virgules des politiques de sécurité TLS à comparer au domaine Amazon. OpensSearch

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

opensearch-in-vpc-only

Vérifie si les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (VPC). La règle est NON_COMPLIANT si un point de terminaison OpenSearch du domaine de service est public.

> **Note**
>
> La règle n'évalue pas les domaines Elasticsearch.

Identificateur : OPENSEARCH_IN_VPC_ONLY

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

opensearch-logs-to-cloudwatch

Vérifie si les domaines Amazon OpenSearch Service sont configurés pour envoyer des journaux à Amazon CloudWatch Logs. La règle est NON_COMPLIANT si la journalisation n'est pas configurée.

> **Note**
>
> La règle n'évalue pas les domaines Elasticsearch.

Identificateur : OPENSEARCH_LOGS_TO_CLOUDWATCH

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

logTypes (facultatif), Type : CSV

Liste des journaux activés, séparés par des virgules. Les valeurs valides sont « search », « index » et « error ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

opensearch-node-to-node-encryption-check

Vérifiez si les nœuds Amazon OpenSearch Service sont chiffrés de bout en bout. La règle est NON_COMPLIANT si le node-to-node chiffrement n'est pas activé sur le domaine

> **Note**
>
> La règle n'évalue pas les domaines Elasticsearch.

Identificateur : OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

opensearch-primary-node-fault-tolerance

Vérifie si les domaines Amazon OpenSearch Service sont configurés avec au moins trois nœuds principaux dédiés. La règle est NON_COMPLIANT pour un domaine de OpenSearch service si « DedicatedMaster Enabled » est défini sur « false » ou si « DedicatedMaster Count » est inférieur à 3.

Identifiant : OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

opensearch-update-check

Vérifie si les mises à jour OpenSearch de version d'Amazon Service sont disponibles mais ne sont pas installées. La règle est NON_COMPLIANT pour un OpenSearch domaine si les dernières mises à jour logicielles ne sont pas installées.

Identificateur : OPENSEARCH_UPDATE_CHECK

Types de ressources : AWS::OpenSearch::Domain

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

rds-aurora-mysql-audit-logging-enabled

Vérifie si les clusters Amazon Aurora MySQL Edition sont configurés pour publier des journaux d'audit sur Amazon Logs. CloudWatch La règle est NON_COMPLIANT si la publication de journaux d'audit n'est pas configurée sur les clusters Amazon Aurora compatibles MySQL.

Identificateur : RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

rds-automatic-minor-version-upgrade-enabled

Vérifie si les instances de base de données Amazon Relational Database Service (Amazon RDS) sont configurées pour les mises à niveau automatiques des versions mineures. La règle est NON_COMPLIANT si la valeur de « auto MinorVersion Upgrade » est fausse.

Identificateur : RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

* Pour plus d'informations sur les valeurs valides pour ces entrées, voir AutoMinorVersionUpgrade Engine dans le guide de AWS CloudFormation l'utilisateur.

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-cluster-auto-minor-version-upgrade-enable

Vérifie si les mises à niveau automatiques des versions mineures sont activées pour les déploiements de clusters Amazon RDS Multi-AZ. La règle est NON_COMPLIANT si autoMinorVersion Upgrade est défini sur false.

Identificateur : RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-cluster-default-admin-check

Vérifie si le nom d'utilisateur de l'administrateur a été modifié par rapport à sa valeur par défaut dans un cluster de base de données Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si le nom d'utilisateur de l'administrateur est défini sur la valeur par défaut.

Identificateur : RDS_CLUSTER_DEFAULT_ADMIN_CHECK

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

valide AdminUserNames (facultatif), Type : CSV

> Liste des noms d'utilisateur d'administrateur séparés par des virgules, susceptibles d'être utilisés par les clusters Amazon RDS. Impossible d'inclure « postgres » ou « admin » comme nom d'utilisateur valide car il s'agit des valeurs par défaut.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-cluster-deletion-protection-enabled

Vérifie si la protection contre la suppression est activée sur un Cluster Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si la protection contre la suppression n'est pas activée sur un cluster Amazon RDS.

Identificateur : RDS_CLUSTER_DELETION_PROTECTION_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

rds-cluster-encrypted-at-rest

Vérifie si un Cluster Amazon Relational Database Service (Amazon RDS) est chiffré au repos. La règle est NON_COMPLIANT si un cluster Amazon RDS n'est pas chiffré au repos.

Identificateur : RDS_CLUSTER_ENCRYPTED_AT_REST

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-cluster-iam-authentication-enabled

Vérifie si l'authentification Identity and Access Management (IAM) AWS est activée sur un cluster Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si l'authentification IAM n'est pas activée sur un cluster Amazon RDS.

Identificateur : RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-cluster-multi-az-enabled

Vérifie si la réplication entre plusieurs zones de disponibilité (multi-AZ) est activée sur les clusters Amazon Aurora et Hermes gérés par Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si une instance Amazon RDS n'est pas configurée avec multi-AZ.

Identificateur : RDS_CLUSTER_MULTI_AZ_ENABLED

Types de ressources : AWS::RDS::DBCluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-db-security-group-not-allowed

Vérifie si des groupes de sécurité de base de données Amazon Relational Database Service (Amazon RDS) n'appartiennent pas au groupe de sécurité de base de données par défaut. La règle est NON_COMPLIANT si des groupes de sécurité de base de données n'appartiennent pas au groupe de sécurité de base de données par défaut.

Identificateur : RDS_DB_SECURITY_GROUP_NOT_ALLOWED

Types de ressources : AWS : :RDS : :DB SecurityGroup

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans les régions Europe (Irlande), Amérique du Sud (São Paulo), USA Est (Virginie du Nord), Asie-Pacifique (Tokyo), USA Ouest (Oregon), USA Ouest (Californie du Nord), Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-enhanced-monitoring-enabled

Vérifie si la surveillance améliorée est activée pour les instances Amazon RDS. Cette règle est NON_COMPLIANT si « `monitoringInterval` » présente la valeur « 0 » dans l'élément de

configuration de l'instance RDS ou si « `monitoringInterval` » ne correspond pas à la valeur du paramètre de la règle.

Identificateur : RDS_ENHANCED_MONITORING_ENABLED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

monitoringInterval (facultatif), Type : int

> Valeur entière, en secondes, entre les points lors de la collecte de métriques de surveillance améliorée pour l'instance de base de données. Les valeurs valides sont 1, 5, 10, 15, 30 et 60.

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* Pour plus d'informations sur les valeurs valides pour ces entrées, voir MonitoringIntervalEngine dans le guide de AWS CloudFormation l'utilisateur.

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-instance-default-admin-check

Vérifie si le nom d'utilisateur de l'administrateur a été modifié par rapport à sa valeur par défaut dans une base de données Amazon Relational Database Service (Amazon RDS). Cette règle ne s'exécutera que sur les instances de base de données RDS. La règle est NON_COMPLIANT si le nom d'utilisateur de l'administrateur est défini sur la valeur par défaut.

Identificateur : RDS_INSTANCE_DEFAULT_ADMIN_CHECK

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

valide AdminUserNames (facultatif), Type : CSV

> Liste des noms d'utilisateur d'administrateur séparés par des virgules, susceptibles d'être utilisés par les instances Amazon RDS. (Impossible d'inclure « postgres » ou « admin » comme nom d'utilisateur valide car il s'agit des valeurs par défaut.)

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

rds-instance-deletion-protection-enabled

Vérifie si la protection contre la suppression est activée sur une instance Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si la protection contre la suppression n'est pas activée sur une instance Amazon RDS (le paramètre DeletionProtection peut par exemple être défini sur false).

> **Warning**
>
> Certaines instances de base de données RDS au sein d'un cluster (Aurora/DocumentDB) seront considérées comme non conformes.

Identificateur : RDS_INSTANCE_DELETION_PROTECTION_ENABLED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

databaseEngines (facultatif), Type : CSV

Liste des moteurs de base de données RDS séparés par des virgules, devant être inclus dans l'évaluation de la règle. Par exemple, « mysql, postgres, mariadb ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

rds-instance-iam-authentication-enabled

Vérifie si l'authentification Identity and Access Management (IAM) AWS est activée sur une instance Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si l'authentification IAM n'est pas activée sur une instance Amazon RDS.

> **Note**
>
> Le moteur de base de données doit être « mysql », « postgres », « aurora », « aurora-mysql » ou « aurora-postgresql ». L'état de l'instance de base de données doit être « available », « backing-up », « storage-optimization » ou « storage-full ».

Identificateur : RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-instance-public-access-check

Vérifie si les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiquement accessibles. La règle est NON_COMPLIANT si le champ publiclyAccessible présente la valeur true dans l'élément de configuration de l'instance.

Identificateur : RDS_INSTANCE_PUBLIC_ACCESS_CHECK

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-in-backup-plan

Vérifie si les bases de données Amazon Relational Database Service (Amazon RDS) sont présentes dans les plans de AWS sauvegarde. La règle est NON_COMPLIANT si les bases de données Amazon RDS ne sont incluses dans aucun plan de sauvegarde AWS .

> **Note**
>
> La règle s'applique uniquement aux instances de base de données Amazon Aurora. Les clusters de base de données ne sont pas pris en charge.

Identificateur : RDS_IN_BACKUP_PLAN

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans l'instance Amazon RDS.

Identificateur : RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des instances Amazon RDS pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID de l'instance Amazon RDS pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

rds-logging-enabled

Vérifie si les journaux respectifs d'Amazon Relational Database Service (Amazon RDS) sont activés. La règle est NON_COMPLIANT si aucun type de journal n'est activé.

> **Note**
>
> Les instances de base de données dont l'état n'est pas « available », « backing-up », « storage-optimization » ou « storage-full » sont évaluées comme `NOT_APPLICABLE`.

Identificateur : RDS_LOGGING_ENABLED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

additionalLogs (facultatif), Type : StringMap

Liste de noms de moteurs et de noms de types de journaux séparés par des virgules. Par exemple, « AdditionalLogs » : « oracle: general, slowquery ; aurora: alert, slowquery »

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir Création de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-meets-restore-time-target

Vérifie si la durée de restauration des instances Amazon Relational Database Service (Amazon RDS) est conforme à la durée spécifiée. La règle est NON_COMPLIANT si la durée LatestRestoreExecutionTimeMinutes d'une instance Amazon RDS est supérieure à quelques minutes. maxRestoreTime

Identifiant : RDS_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balises des instances Amazon RDS pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

ID de l'instance Amazon RDS pour la règle à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-multi-az-support

Vérifie si la haute disponibilité est activée pour vos instances de base de données RDS.

Dans un déploiement multi-AZ, Amazon RDS fournit et maintient automatiquement un réplica de secours synchrone dans une autre zone de disponibilité. Pour en savoir plus, veuillez consulter la section Haute disponibilité (Multi-AZ) dans le Guide de l'utilisateur Amazon RDS.

> **Note**
> Cette règle n'évalue pas les instances de base de données Amazon Aurora, Amazon DocumentDB et Amazon Neptune.

Identificateur : RDS_MULTI_AZ_SUPPORT

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode

proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* Pour plus d'informations sur les valeurs valides pour ces entrées, voir MultiAZ et Engine dans le guide de l' AWS CloudFormation utilisateur.

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-resources-protected-by-backup-plan

Vérifie si les instances Amazon Relational Database Service (Amazon RDS) sont protégées par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué à l'instance de base de données Amazon RDS.

Identificateur : RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

> Balise des instances Amazon RDS pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID de l'instance Amazon RDS pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-snapshots-public-prohibited

Vérifie si les instantanés Amazon Relational Database Service (Amazon RDS) sont publics. La règle est NON_COMPLIANT si des instantanés Amazon RDS nouveaux ou existants sont publics.

> **Note**
>
> La saisie des résultats de conformité peut prendre jusqu'à 12 heures.

Identificateur : RDS_SNAPSHOTS_PUBLIC_PROHIBITED

Types de ressources : AWS : :RDS : :DBSnapshot, AWS : :RDS : :DB ClusterSnapshot

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-snapshot-encrypted

Vérifie si les instantanés de base de données Amazon Relational Database Service (Amazon RDS) sont chiffrés. La règle est NON_COMPLIANT, si les instantanés de bases de données Amazon RDS ne sont pas chiffrés.

Identificateur : RDS_SNAPSHOT_ENCRYPTED

Types de ressources : AWS : :RDS : :DBSnapshot, AWS : :RDS : :DB ClusterSnapshot

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

rds-storage-encrypted

Vérifie si le chiffrement du stockage est activé pour vos instances de base de données Amazon Relational Database Service (Amazon RDS). La règle est NON_COMPLIANT si le chiffrement du stockage n'est pas activé.

Identificateur : RDS_STORAGE_ENCRYPTED

Types de ressources : AWS::RDS::DBInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyId (Facultatif), Type : chaîne

ID de clé KMS ou Amazon Resource Name (ARN) utilisé pour chiffrer le stockage.

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

redshift-audit-logging-enabled

Vérifie si les clusters Amazon Redshift journalisent les audits dans un compartiment spécifique. La règle est NON_COMPLIANT si la journalisation des audits n'est pas activée sur un cluster Redshift ou si le paramètre « `bucketNames` » est fourni sans que la destination de journalisation des audits ne corresponde.

Identificateur : REDSHIFT_AUDIT_LOGGING_ENABLED

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

bucketNames (facultatif), Type : CSV

Liste des noms de compartiments Amazon S3 séparés par des virgules pour le stockage des journaux d'audit.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

redshift-backup-enabled

Vérifie si les instantanés automatisés Amazon Redshift sont activés pour les clusters. La règle est NON_COMPLIANT si la valeur de `automatedSnapshotRetentionPeriod` est supérieure à `MaxRetentionPeriod` ou inférieure à `MinRetentionPeriod` ou si la valeur est égale à 0.

Identificateur : REDSHIFT_BACKUP_ENABLED

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

MinRetentionPeriod (Facultatif), Type : int

Valeur minimale pour la période de conservation. La valeur minimum est de 1.

MaxRetentionPeriod (Facultatif), Type : int

Valeur maximale pour la période de conservation. La valeur maximale est 35.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

redshift-cluster-configuration-check

Vérifie si les clusters Amazon Redshift présentent les paramètres spécifiés. La règle est NON_COMPLIANT si le cluster Amazon Redshift n'est pas chiffré ou chiffré avec une autre clé, ou si la journalisation des audits n'est pas activée sur un cluster.

Identificateur : REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

grappe DbEncrypted, Type : valeur booléenne, Valeur par défaut : true

Le chiffrement de base de données est activé.

loggingEnabled, Type : valeur booléenne, Valeur par défaut : true

La journalisation d'audit est activée.

nodeTypes (facultatif), Type : CSV, Valeur par défaut : dc1.large

Spécifiez le type de nœud.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

redshift-cluster-kms-enabled

Vérifie si les clusters Amazon Redshift utilisent une clé spécifiée AWS Key Management Service (AWS KMS) pour le chiffrement. La règle est COMPLIANT si le chiffrement est activé et si le cluster

est chiffré avec la clé fournie dans le paramètre `kmsKeyArn`. La règle est NON_COMPLIANT si le cluster n'est pas chiffré ou chiffré avec une autre clé.

Identificateur : REDSHIFT_CLUSTER_KMS_ENABLED

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

Liste séparée par des virgules des AWS KMS principaux noms de ressources Amazon (ARN) utilisés dans les clusters Amazon Redshift pour le chiffrement.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

redshift-cluster-maintenancesettings-check

Vérifie si les clusters Amazon Redshift présentent les paramètres de maintenance spécifiés. La règle est NON_COMPLIANT si les mises à niveau automatiques vers la version majeure sont désactivées.

Identificateur : REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

autoriser VersionUpgrade, Type : valeur booléenne, Valeur par défaut : true

L'autorisation de mise à niveau de la version est activée.

preferredMaintenanceWindow (Facultatif), Type : chaîne

Fenêtre de maintenance planifiée pour les clusters (par exemple, Lun:09:30-Lun:10:00).

automatisé SnapshotRetentionPeriod (facultatif), Type : int, Valeur par défaut : 1

Nombre de jours de conservation des instantanés automatiques.

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* Pour plus d'informations sur les valeurs valides de ces entrées AutomatedSnapshotRetentionPeriod, reportez-vous aux sections PreferredMaintenanceFenêtre et AllowVersionMise à niveau du guide de AWS CloudFormation l'utilisateur.

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

redshift-cluster-public-access-check

Vérifie si les clusters Amazon Redshift ne sont pas publiquement accessibles. La règle est NON_COMPLIANT si le champ publiclyAccessible présente la valeur true dans l'élément de configuration du cluster.

Identificateur : REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

redshift-default-admin-check

Vérifie si le nom d'utilisateur de l'administrateur a été modifié par rapport à sa valeur par défaut dans un cluster Amazon Redshift. La règle est NON_COMPLIANT si le nom d'utilisateur de l'administrateur d'un cluster Redshift est défini sur « awsuser » ou s'il ne correspond pas à la valeur indiquée dans le paramètre.

Identificateur : REDSHIFT_DEFAULT_ADMIN_CHECK

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

valide AdminUserNames (facultatif), Type : CSV

Liste des noms d'utilisateur d'administrateur séparés par des virgules devant être utilisés par les clusters Redshift. Remarque : « awsuser » est la valeur par défaut et n'est pas acceptée.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

redshift-default-db-name-check

Vérifie si le nom de la base de données a été modifié par rapport à sa valeur par défaut dans un cluster Redshift. La règle est NON_COMPLIANT si le nom de la base de données d'un cluster Redshift est défini sur « dev », ou si le paramètre facultatif est fourni et s'il ne correspond pas au nom de la base de données.

Identificateur : REDSHIFT_DEFAULT_DB_NAME_CHECK

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

validDatabaseNames (Facultatif), Type : CSV

Liste des noms de bases de données séparés par des virgules pour les clusters Redshift.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

redshift-enhanced-vpc-routing-enabled

Vérifie si l'option « améliorée » VpcRouting est activée sur le cluster Amazon Redshift. La règle est NON_COMPLIANT si le paramètre « amélioré VpcRouting » n'est pas activé ou si la configuration est configurée. enhancedVpcRouting le champ est « faux ».

Identificateur : REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

redshift-require-tls-ssl

Vérifie si les clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. La règle est NON_COMPLIANT si le paramètre require_SSL d'un cluster Amazon Redshift n'est pas défini sur true.

Identificateur : REDSHIFT_REQUIRE_TLS_SSL

Types de ressources : AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter Groupe

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

accès au port non restreint par redshift

Vérifie si les groupes de sécurité associés à un cluster Amazon Redshift ont des règles entrantes qui autorisent le trafic entrant sans restriction. La règle est NON_COMPLIANT s'il existe des règles entrantes qui autorisent un trafic entrant illimité vers le port du cluster Redshift.

Identifiant : REDSHIFT_UNRESTRICTED_PORT_ACCESS

Types de ressources : AWS::Redshift::Cluster

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

required-tags

Vérifie si vos ressources ont les balises que vous spécifiez. Par exemple, vous pouvez vérifier si vos instances Amazon EC2 présentent la balise `CostCenter`, tout en vérifiant si toutes vos instances RDS sont associées à un ensemble de balises Keys. S'il y a plusieurs valeurs, séparez-les à l'aide de virgules. Vous pouvez vérifier jusqu'à 6 balises à la fois.

Le document AWS Systems Manager d'automatisation AWS géré `AWS-SetRequiredTags` ne fonctionne pas comme une correction avec cette règle. Vous devrez créer votre propre documentation personnalisée sur l'automatisation Systems Manager à des fins de correction.

Contexte : AWS permet d'attribuer des métadonnées aux AWS ressources sous forme de balises. Chaque balise est une étiquette composée d'une clé et d'une valeur facultative qui permettent de

stocker des informations sur la ressource ou les données conservées sur cette ressource. Pour plus d'informations, consultez Créer votre stratégie de balisage.

Vous pouvez utiliser cette règle pour rechercher les ressources de votre compte qui n'ont pas été lancées avec les configurations souhaitées en spécifiant les ressources qui doivent présenter des balises et la valeur attendue pour chaque balise. Vous pouvez également appliquer des mesures correctives pour remédier aux erreurs de balisage. Néanmoins, cette règle n'empêche pas la création de ressources présentant des balises incorrectes.

Identificateur : REQUIRED_TAGS

Types de ressources AWS::ACM::Certificate, AWS::AutoScaling : : : AutoScaling Groupe, AWS::CloudFormation::Stack, AWS::CodeBuild ::Project, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl,, AWS::EC2::NetworkInterface AWS::EC2::RouteTable AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoad Équilibrage : : LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription,, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter Groupe, AWS::Redshift::ClusterSecurity Groupe AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnet Groupe, AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

tag1Key, Type : chaîne, Par défaut : CostCenter

Clé de la balise requise.

tag1Value (facultatif), Type : CSV

Valeur optionnelle de la balise requise. S'il y a plusieurs valeurs, séparez-les à l'aide de virgules.

tag2Key (facultatif), Type : chaîne

Clé d'une deuxième balise requise.

tag2Value (facultatif), Type : CSV

Valeur optionnelle de la deuxième balise requise. S'il y a plusieurs valeurs, séparez-les à l'aide de virgules.

tag3Key (facultatif), Type : chaîne

Clé de la troisième balise requise.

tag3Value (facultatif), Type : CSV

Valeur optionnelle de la troisième balise requise. S'il y a plusieurs valeurs, séparez-les à l'aide de virgules.

tag4Key (facultatif), Type : chaîne

Clé de la quatrième balise requise.

tag4Value (facultatif), Type : CSV

Valeur optionnelle de la quatrième balise requise. S'il y a plusieurs valeurs, séparez-les à l'aide de virgules.

tag5Key (facultatif), Type : chaîne

Clé de la cinquième balise requise.

tag5Value (facultatif), Type : CSV

Valeur optionnelle de la cinquième balise requise. S'il y a plusieurs valeurs, séparez-les à l'aide de virgules.

tag6Key (facultatif), Type : chaîne

Clé de la sixième balise requise.

tag6Value (facultatif), Type : CSV

Valeur optionnelle de la sixième balise requise. S'il y a plusieurs valeurs, séparez-les à l'aide de virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir Création de règles gérées AWS Config avec des modèles AWS CloudFormation.

restricted-common-ports

> **Important**
>
> L'identifiant (RESTRICTED_INCOMING_TRAFFIC) et le nom (restricted-common-ports) de cette règle sont différents.

Vérifie si les groupes de sécurité en cours d'utilisation interdisent le trafic TCP (Transmission Control Protocol) entrant illimité vers les ports spécifiés. La règle est COMPLIANT si :

- L'accès au port est bloqué pour l'ensemble du trafic TCP.
- L'accès aux ports est ouvert au trafic TCP par le biais de règles entrantes, dont la source est soit une adresse IPv4 unique, soit une plage d'adresses IPv4 en notation CIDR qui ne couvre pas toutes les adresses IPv4 (« 0.0.0.0/0 »).
- L’accès aux ports est ouvert au trafic TCP par le biais de règles entrantes, dont la source est soit une adresse IPv6 unique, soit une plage d’adresses IPv6 en notation CIDR qui ne couvre pas toutes les adresses IPv6 (« ::/0) »).

La règle est NON_COMPLIANT si les adresses IP des connexions TCP entrantes ne sont pas limitées aux ports spécifiés.

Identificateur : RESTRICTED_INCOMING_TRAFFIC

Types de ressources : AWS::EC2::SecurityGroup

Type de déclencheur : modifications de configuration et périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

blockedPort1 (facultatif), Type : int, Valeur par défaut : 20

Numéro du port TCP bloqué. La valeur par défaut « 20 » correspond au transfert de données FTP (File Transfer Protocol).

blockedPort2 (facultatif), Type : int, Valeur par défaut : 21

Numéro du port TCP bloqué. La valeur par défaut « 21 » correspond au contrôle de commande FTP (File Transfer Protocol).

blockedPort3 (facultatif), Type : int, Valeur par défaut : 3389

Numéro du port TCP bloqué. La valeur par défaut « 3389 » correspond au protocole RDP (Remote Desktop Protocol).

blockedPort4 (facultatif), Type : int, Valeur par défaut : 3306

Numéro du port TCP bloqué. La valeur par défaut « 3306 » correspond au protocole MySQL.

blockedPort5 (facultatif), Type : int, Valeur par défaut : 4333

Numéro du port TCP bloqué. La valeur par défaut « 4333 » correspond au protocole MySQL.

blockedPorts (facultatif), Type : CSV

Liste de numéros de ports TCP bloqués séparés par des virgules. Par exemple, 20, 21, 3306, 3389 et 4333.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

root-account-hardware-mfa-enabled

Vérifie si votre AWS compte est activé pour utiliser un dispositif matériel d'authentification multifactorielle (MFA) pour se connecter avec les informations d'identification root. La règle est NON_COMPLIANT si tous les périphériques MFA virtuels sont autorisés à se connecter avec des informations d'identification racines.

> **Note**
>
> Règles gérées et types de ressources IAM globaux
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`AWS::IAM::Role, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.
> Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des

évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.
Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

root-account-mfa-enabled

Vérifie si l'utilisateur root de votre AWS compte nécessite une authentification multifactorielle pour se connecter à la console. La règle est NON_COMPLIANT si l'utilisateur du compte root AWS Identity and Access Management (IAM) n'a pas activé l'authentification multifactorielle (MFA).

> **Note**
>
> Règles gérées et types de ressources IAM globaux
> Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.
Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Identificateur : ROOT_ACCOUNT_MFA_ENABLED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

route53-query-logging-enabled

Vérifie si la journalisation des requêtes DNS est activée pour les zones hébergées publiques Amazon Route 53. La règle est NON_COMPLIANT si la journalisation des requêtes DNS n'est pas activée pour les zones hébergées publiques Amazon Route 53.

Identificateur : ROUTE53_QUERY_LOGGING_ENABLED

Types de ressources : AWS::Route53::HostedZone

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-access-point-in-vpc-only

Vérifie si un point d'accès Amazon S3 n'autorise pas l'accès depuis Internet (NetworkOrigin c'est un VPC). La règle est NON_COMPLIANT s'il s' NetworkOrigin agit d'Internet.

Identificateur : S3_ACCESS_POINT_IN_VPC_ONLY

Types de ressources : AWS::S3::AccessPoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-access-point-public-access-blocks

Vérifie si les paramètres de blocage de l'accès public sont activés sur les points d'accès Amazon S3. La règle est NON_COMPLIANT si les paramètres de blocage de l'accès public ne sont pas activés sur les points d'accès S3.

Identificateur : S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

Types de ressources : AWS::S3::AccessPoint

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

excludedAccessPoints (Facultatif), Type : CSV

Liste de noms séparés par des virgules pour les points d'accès publics Amazon S3 autorisés.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-account-level-public-access-blocks

Vérifie si les paramètres de bloc d'accès public requis sont configurés au niveau du compte. La règle est NON_COMPLIANT uniquement lorsque les champs définis ci-dessous ne correspondent pas aux champs correspondants dans l'élément de configuration.

> **Note**
>
> Si vous utilisez cette règle, vérifiez que le bloc d'accès public S3 est activé. La règle est déclenchée par des modifications, elle ne sera donc invoquée que si le bloc d'accès public S3 est activé. Si le bloc d'accès public S3 n'est pas activé, la règle renvoie INSUFFICIENT_DATA. Si c'est le cas, il se peut que certains compartiments soient publics. Pour plus d'informations sur le bloc d'accès public S3, consultez Blocage de l'accès public à votre stockage Amazon S3.

Identificateur : S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

Types de ressources : AWS::S3::AccountPublic AccessBlock

Type de déclencheur : modifications de configuration (état actuel non vérifié, évalué uniquement lorsque les modifications génèrent de nouveaux événements)

> **Note**
>
> Cette règle n'est déclenchée que par des modifications de configuration pour la région spécifique où se trouve le point de terminaison S3. La règle est vérifiée périodiquement

dans toutes les autres régions. Un délai peut être nécessaire avant que la règle ne renvoie NON_COMPLIANT si une modification a été apportée dans une autre région.

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

IgnorePublicAcls (Facultatif), Type : chaîne, Valeur par défaut : True

IgnorePublicAcls est appliqué ou non, valeur par défaut True

BlockPublicPolicy (Facultatif), Type : chaîne, Valeur par défaut : True

BlockPublicPolicy est appliqué ou non, valeur par défaut True

BlockPublicAcls (Facultatif), Type : chaîne, Valeur par défaut : True

BlockPublicAcls est appliqué ou non, valeur par défaut True

RestrictPublicBuckets (Facultatif), Type : chaîne, Valeur par défaut : True

RestrictPublicBuckets est appliqué ou non, valeur par défaut True

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

s3-account-level-public-access-blocks-periodic

Vérifie si les paramètres de bloc d'accès public requis sont configurés au niveau du compte. La règle est NON_COMPLIANT si l'élément de configuration ne correspond pas à une ou plusieurs configurations définies dans les paramètres (ou par défaut).

Identificateur : S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

IgnorePublicAcls (Facultatif), Type : chaîne

IgnorePublicAcls est appliqué ou non, valeur par défaut True

BlockPublicPolicy (Facultatif), Type : chaîne

BlockPublicPolicy est appliqué ou non, valeur par défaut True

BlockPublicAcls (Facultatif), Type : chaîne

BlockPublicAcls est appliqué ou non, valeur par défaut True

RestrictPublicBuckets (Facultatif), Type : chaîne

RestrictPublicBuckets est appliqué ou non, valeur par défaut True

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-acl-prohibited

Vérifie si les compartiments Amazon Simple Storage Service (Amazon S3) acceptent les autorisations utilisateur par le biais de listes de contrôle d'accès (ACL). La règle est NON_COMPLIANT si l'accès des utilisateurs est configuré dans les listes ACL des compartiments Amazon S3.

Identificateur : S3_BUCKET_ACL_PROHIBITED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-blacklisted-actions-prohibited

Vérifie si une politique de compartiment Amazon Simple Storage Service (Amazon S3) n'autorise pas les actions bloquées au niveau du compartiment et au niveau de l'objet sur les ressources du compartiment pour les principaux d'autres comptes. AWS Par exemple, la règle vérifie que la politique du compartiment Amazon S3 n'autorise aucun autre AWS compte à effectuer `s3:GetBucket*` des actions `s3:DeleteObject` sur aucun objet du compartiment. La règle est NON_COMPLIANT si des actions figurant sur la liste de blocage sont autorisées par la politique de compartiment Amazon S3.

> **Note**
>
> La règle vérifie uniquement les entités de la propriété Principal et ne prend pas en compte les conditions liées à la propriété Condition dans une politique

Identificateur : S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

sur liste noire ActionPattern, Type : CSV

Liste séparée par des virgules de modèles d'action sur liste noire, par exemple, s3 : GetBucket * et s3 :. DeleteObject

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

Activé pour la réplication entre régions du compartiment S3

Vérifie si vous avez activé la réplication entre régions S3 pour vos compartiments Amazon S3. La règle est NON_COMPLIANT si aucune règle de réplication n'est activée pour la réplication entre régions.

Identifiant : S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-default-lock-enabled

Vérifie si le verrouillage du compartiment S3 est activé par défaut. La règle est NON_COMPLIANT si le verrouillage n'est pas activé.

Identificateur : S3_BUCKET_DEFAULT_LOCK_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

mode (facultatif), Type : chaîne

> mode : (facultatif) : paramètre de mode avec des valeurs valides GOVERNANCE ou COMPLIANCE.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-level-public-access-prohibited

Vérifie si les compartiments S3 sont publiquement accessibles. La règle est NON_COMPLIANT si aucun compartiment S3 n'est indiqué dans le paramètre `excludedPublicBuckets` et si les paramètres au niveau du compartiment sont publics.

Identificateur : S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

excludedPublicBuckets (Facultatif), Type : CSV

Liste des noms de compartiments publics Amazon S3 autorisés, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

s3-bucket-logging-enabled

Vérifie si la journalisation est activée pour vos compartiments S3. La règle est NON_COMPLIANT si la journalisation n'est pas activée.

Identificateur : S3_BUCKET_LOGGING_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

targetBucket (facultatif), Type : chaîne

Compartiment S3 cible pour stocker les journaux d'accès au serveur.

targetPrefix (facultatif), Type : chaîne

Préfixe du compartiment S3 pour stocker les journaux d'accès au serveur.

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "BucketName": "my-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "my-log-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-mfa-delete-enabled

Vérifie si la suppression MFA est activée dans la configuration de la gestion des versions du compartiment Amazon Simple Storage Service (Amazon S3). La règle est NON_COMPLIANT si la suppression MFA n'est pas activée.

Identificateur : S3_BUCKET_MFA_DELETE_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

s3-bucket-policy-grantee-check

Vérifie que l'accès accordé par le compartiment Amazon S3 est restreint par AWS les principaux, les utilisateurs fédérés, les principaux de service, les adresses IP ou les VPC que vous fournissez. La règle est COMPLIANT si une stratégie de compartiment n'est pas présente.

Par exemple, si le paramètre d'entrée pour la règle est la liste des deux principaux : `111122223333` et `444455556666` et la politique de compartiment spécifie que seul `111122223333` peut accéder au compartiment, alors la règle est COMPLIANT. Avec les mêmes paramètres d'entrée : si la politique de compartiment spécifie que `111122223333` et `444455556666` peuvent accéder au compartiment, elle est également conforme. Toutefois, si la politique de compartiment spécifie que `999900009999` peut accéder au compartiment, la règle est NON-COMPLIANT.

> **Note**
>
> Si une politique de compartiment contient plusieurs instructions, chaque instruction de la politique de compartiment est évaluée par cette règle.

Identificateur : S3_BUCKET_POLICY_GRANTEE_CHECK

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

awsPrincipals (facultatif), Type : CSV

Liste de principes séparés par des virgules, tels que les ARN des utilisateurs IAM, les ARN des rôles IAM et les AWS comptes, par exemple « arn:aws:iam : :111122223333:User/Alice, arn:aws:iam : :444455556666:role/bob, 123456789012 ».

servicePrincipals (facultatif), Type : CSV

Liste des principaux de services séparés par des virgules, par exemple « cloudtrail.amazonaws.com, lambda.amazonaws.com ».

federatedUsers (facultatif), Type : CSV

Liste de fournisseurs d'identité séparés par des virgules pour la fédération d'identité Web tels qu'Amazon Cognito et les fournisseurs d'identité SAML. Par exemple, « cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider ».

ipAddresses (facultatif), Type : CSV

Liste d'adresses IP au format CIDR séparées par des virgules, par exemple « 10.0.0.1, 192.168.1.0/24, 2001:db8::/32 ».

vpcIds (facultatif), Type : CSV

Liste des identifiants des réseaux Amazon Virtual Private Clouds (Amazon VPC) séparés par des virgules, par exemple « vpc-1234abc0, vpc-ab1234c0 ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

s3-bucket-policy-not-more-permissive

Vérifie que vos politiques de compartiment Amazon Simple Storage Service n'autorisent pas d'autres autorisations entre comptes que la politique de compartiment de contrôle Amazon S3 que vous fournissez.

> **Note**
>
> Si vous fournissez une valeur de paramètre non valide, vous obtenez l'erreur suivante : la valeur pour le paramètre controlPolicy doit être une politique de compartiment Amazon S3.

Identificateur : S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

controlPolicy, Type : chaîne

Politique de compartiment Amazon S3 qui définit une limite supérieure sur les autorisations de vos compartiments S3. La politique peut avoir une longueur de 1 024 caractères au maximum.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

s3-bucket-public-read-prohibited

Vérifie que vos compartiments Amazon S3 n'autorisent pas un accès public en lecture. La règle vérifie les paramètres de blocage d'accès public , la stratégie de compartiment et la liste de contrôle d'accès (ACL) du compartiment.

La règle est conforme lorsque les deux conditions suivantes sont réunies :

- Le paramètre de blocage d'accès public limite les politiques publiques ou la politique de compartiment n'autorise pas l'accès public en lecture.
- Le paramètre de blocage d'accès public limite les listes ACL publiques ou la liste ACL de compartiment n'autorise pas l'accès public en lecture.

La règle n’est pas conforme dans les cas suivants :

- Si le paramètre Bloquer l'accès public ne restreint pas les politiques publiques, AWS Config évalue si la politique autorise l'accès public en lecture. Si la politique autorise un accès public en lecture, la règle n'est pas conforme.

- Si le paramètre Bloquer l'accès public ne restreint pas les ACL du bucket public, AWS Config évalue si l'ACL du bucket autorise l'accès public en lecture. Si la liste ACL de compartiment autorise un accès public en lecture, la règle n'est pas conforme.

Identificateur : S3_BUCKET_PUBLIC_READ_PROHIBITED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : modifications de configuration et périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-public-write-prohibited

Vérifie que vos compartiments Amazon S3 n'autorisent pas l'accès public en écriture. La règle vérifie les paramètres de blocage d'accès public , la stratégie de compartiment et la liste de contrôle d'accès (ACL) du compartiment.

La règle est conforme lorsque les deux conditions suivantes sont réunies :

- Le paramètre de blocage d'accès public limite les politiques publiques ou la politique de compartiment n'autorise pas l'accès public en écriture.
- Le paramètre de blocage d'accès public limite les listes ACL publiques ou la liste ACL de compartiment n'autorise pas l'accès public en écriture.

La règle n’est pas conforme dans les cas suivants :

- Si le paramètre Bloquer l'accès public ne restreint pas les politiques publiques, AWS Config évalue si la politique autorise l'accès public en écriture. Si la politique autorise un accès public en écriture, la règle n'est pas conforme.

- Si le paramètre Bloquer l'accès public ne limite pas les ACL du bucket public, AWS Config évalue si l'ACL du bucket autorise l'accès public en écriture. Si la liste ACL de compartiment autorise un accès public en écriture, la règle n'est pas conforme.

> **Note**
>
> Cette règle n'évalue pas les modifications apportées au blocage de l'accès public au niveau du compte. Pour vérifier si les paramètres de blocage d'accès public requis sont configurés au niveau du compte, consultez s3-account-level-public-access-blocks et s3-account-level-public-access-blocks-periodic.

Identificateur : S3_BUCKET_PUBLIC_WRITE_PROHIBITED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : modifications de configuration et périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-replication-enabled

Vérifie si les règles de réplication sont activées sur les compartiments S3. La règle est NON_COMPLIANT si un compartiment S3 n'est associé à aucune règle de réplication ou si aucune règle de réplication n'est activée.

Identificateur : S3_BUCKET_REPLICATION_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

ReplicationType (Facultatif), Type : chaîne

Valeurs acceptées : « CROSS-REGION » et « SAME-REGION ». Saisissez « CROSS-REGION » pour vérifier que seule la réplication entre régions est activée pour tous les compartiments. Saisissez « SAME-REGION » pour vérifier que seule la réplication dans une même région est activée pour tous les compartiments.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-server-side-encryption-enabled

Vérifie si le chiffrement par défaut est activé sur votre compartiment Amazon S3 ou si la politique de compartiment Amazon S3 refuse explicitement les requêtes `put-object` sans chiffrement côté serveur, à l'aide d'AES-256 ou de AWS Key Management Service. La règle est NON_COMPLIANT si votre compartiment Amazon S3 n'est pas chiffré par défaut.

Identificateur : S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-bucket-ssl-requests-only

Vérifie si les compartiments S3 présentent des politiques exigeant que les requêtes utilisent SSL/TLS. La règle est NON_COMPLIANT si un compartiment S3 présente des politiques autorisant les requêtes HTTP.

Identificateur : S3_BUCKET_SSL_REQUESTS_ONLY

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

s3-bucket-versioning-enabled

Vérifie si la gestion des versions est activée sur vos compartiments S3. Si vous le souhaitez, la règle vérifie si la suppression MFA est activée sur vos compartiments S3.

Identificateur : S3_BUCKET_VERSIONING_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

est MfaDeleteEnabled (Facultatif), Type : chaîne

La suppression MFA est activée sur vos compartiments S3.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-default-encryption-kms

Vérifie si les compartiments S3 sont chiffrés avec le service de gestion des AWS clés (AWS KMS). La règle est NON_COMPLIANT si le compartiment S3 n'est pas chiffré avec une clé AWS KMS.

Identificateur : S3_DEFAULT_ENCRYPTION_KMS

Types de ressources : AWS::S3::Bucket, AWS::KMS::Key

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

Liste séparée par des virgules des AWS ARN des clés KMS autorisés pour le chiffrement des compartiments Amazon S3.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-event-notifications-enabled

Vérifie si les notifications d'événements Amazon S3 sont activées sur un compartiment S3. La règle est NON_COMPLIANT si les notifications d'événements S3 ne sont pas définies sur un compartiment, ou si le type d'événement ou la destination ne correspondent pas aux paramètres `eventTypes` et destinationArn.

Identificateur : S3_EVENT_NOTIFICATIONS_ENABLED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

destinationArn (facultatif), Type : chaîne

Le nom de ressource Amazon (ARN) de la destination pour la notification d'événement (rubrique Amazon SNS, AWS Lambda, Amazon SQS Queue).

eventTypes (facultatif), Type : CSV

Liste des types d'événements Amazon S3 préférés séparés par des virgules

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

s3-last-backup-recovery-point-created

Vérifie si un point de récupération a été créé pour Amazon Simple Storage Service (Amazon S3). La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans le compartiment Amazon S3.

Identificateur : S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::S3::Bucket

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises du compartiment Amazon S3 pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

Nom du compartiment Amazon S3 pour les règles à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-lifecycle-policy-check

Vérifie si une règle de cycle de vie est configurée pour un compartiment Amazon Simple Storage Service (Amazon S3). La règle est NON_COMPLIANT si aucune règle de configuration du cycle de vie n'est active ou si la configuration ne correspond pas aux valeurs des paramètres.

Identificateur : S3_LIFECYCLE_POLICY_CHECK

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

targetTransitionDays (Facultatif), Type : int

Nombre de jours après la création d'objets lorsque ceux-ci sont transmis à la classe de stockage spécifiée (par exemple, 30 jours).

targetExpirationDays (Facultatif), Type : int

Nombre de jours après la création d'objets lorsque ceux-ci sont supprimés (par exemple, 395 jours).

cible TransitionStorageClass (facultatif), Type : chaîne

Type de classe de stockage de destination (par exemple, Amazon S3 Standard-Infrequent Access [S3 Standard-IA]). Pour en savoir plus, consultez l'adresse https: //docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html.

targetPrefix (facultatif), Type : chaîne

Préfixe d'objet Amazon S3 permettant d'identifier un ou plusieurs objets.

bucketNames (facultatif), Type : CSV

Liste des noms de compartiments Amazon S3 séparés par des virgules pour lesquels la politique de cycle de vie est activée.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-meets-restore-time-target

Vérifie si la durée de restauration des compartiments Amazon Simple Storage Service (Amazon S3) correspond à la durée spécifiée. La règle est NON_COMPLIANT si LatestRestoreExecutionTimeMinutes la durée d'un compartiment Amazon S3 est supérieure maxRestoreTime à quelques minutes.

Identifiant : S3_MEETS_RESTORE_TIME_TARGET

Types de ressources : AWS::S3::Bucket

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum RestoreTime, Type : int

Valeur numérique de la durée maximale autorisée pour la restauration.

resourceTags (facultatif), Type : chaîne

Balises du compartiment Amazon S3 pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

Nom du compartiment Amazon S3 pour les règles à vérifier.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-resources-protected-by-backup-plan

Vérifie si des compartiments Amazon Simple Storage Service (Amazon S3) sont protégés par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué au compartiment Amazon S3.

Identificateur : S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::S3::Bucket

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des compartiments Amazon S3 pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

Nom du compartiment Amazon S3 pour les règles à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

s3-version-lifecycle-policy-check

Vérifie si une politique de cycle de vie est configurée pour les compartiments Amazon Simple Storage Service (Amazon S3) compatibles avec la gestion des versions. La règle est NON_COMPLIANT si la politique de cycle de vie d'Amazon S3 n'est pas activée.

Identificateur : S3_VERSION_LIFECYCLE_POLICY_CHECK

Types de ressources : AWS::S3::Bucket

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

bucketNames (facultatif), Type : CSV

Liste des noms de compartiments Amazon S3 séparés par des virgules pour lesquels la politique de cycle de vie est activée.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sagemaker-endpoint-configuration-kms-key-configured

Vérifie si la AWS clé du service de gestion des clés (AWS KMS) est configurée pour une configuration de point de SageMaker terminaison Amazon. La règle est NON_COMPLIANT si « ID » KmsKey n'est pas spécifié pour la configuration du point de terminaison Amazon SageMaker .

Identificateur : SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

Types de ressources : AWS::SageMaker::EndpointConfig

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : chaîne

Liste séparée par des virgules des ARN de clé AWS KMS spécifiques autorisés pour la configuration d'un point de terminaison Amazon SageMaker .

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sagemaker-endpoint-config-prod-instance-count

Vérifie si les configurations des SageMaker terminaux Amazon ont une valeur supérieure à 1 pour les variantes de production InitialInstance « Count ». La règle est NON_COMPLIANT si le nombre de variantes de production « InitialInstance Count » est égal à 1.

Identifiant : SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

Types de ressources : AWS::SageMaker::EndpointConfig

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sagemaker-notebook-instance-inside-vpc

Vérifie si une instance Amazon SageMaker Notebook est lancée dans un VPC ou dans une liste de sous-réseaux approuvés. La règle est NON_COMPLIANT si une instance de bloc-notes n'est pas lancée dans un réseau VPC ou si son ID de sous-réseau ne figure pas dans la liste des paramètres.

Identificateur : SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

Types de ressources : AWS::SageMaker::NotebookInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

SubnetIds (Facultatif), Type : CSV

Liste des ID de sous-réseau séparés par des virgules dans lesquels les instances de bloc-notes peuvent être lancées.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sagemaker-notebook-instance-kms-key-configured

Vérifie si une AWS clé du service de gestion des clés (AWS KMS) est configurée pour une instance de SageMaker bloc-notes Amazon. La règle est NON_COMPLIANT si « ID » KmsKey n'est pas spécifié pour l'instance de bloc-notes. SageMaker

Identificateur : SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

Types de ressources : AWS::SageMaker::NotebookInstance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : chaîne

Liste séparée par des virgules des ARN de clé AWS KMS autorisés pour une instance de bloc-notes Amazon SageMaker .

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sagemaker-notebook-instance-root-access-check

Vérifie si le SageMaker RootAccess paramètre Amazon est activé pour les instances Amazon SageMaker Notebook. La règle est NON_COMPLIANT si le RootAccess paramètre est défini sur « Activé » pour une instance de SageMaker bloc-notes Amazon.

Identificateur : SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

Types de ressources : AWS::SageMaker::NotebookInstance

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sagemaker-notebook-no-direct-internet-access

Vérifie si l'accès direct à Internet est désactivé pour une instance de SageMaker bloc-notes Amazon. La règle est NON_COMPLIANT si une instance de SageMaker bloc-notes est connectée à Internet.

Identificateur : SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

Types de ressources : AWS::SageMaker::NotebookInstance

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

secretsmanager-rotation-enabled-check

Vérifie si la rotation du secret de AWS Secrets Manager est activée. La règle vérifie également un paramètre facultatif `maximumAllowedRotationFrequency`. Si le paramètre est spécifié, la fréquence de rotation du secret est comparée à la fréquence maximale autorisée. La règle est NON_COMPLIANT si la rotation du secret n'est pas planifiée. La règle est également NON_COMPLIANT si la fréquence de rotation est supérieure au nombre spécifié dans le paramètre maximumAllowedRotation Frequency.

> **Note**
>
> Réévaluer cette règle dans un délai de 4 heures après la première évaluation n'aura aucun effet sur les résultats.

Identificateur : SECRETSMANAGER_ROTATION_ENABLED_CHECK

Types de ressources : AWS::SecretsManager::Secret

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

maximum AllowedRotationFrequency (facultatif), Type : int

Fréquence de rotation maximale autorisée du secret en jours.

maximum AllowedRotationFrequencyInHours (facultatif), Type : int

Fréquence de rotation maximale autorisée du secret en heures.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

secretsmanager-scheduled-rotation-success-check

Vérifie si AWS les secrets de Secrets Manager ont été correctement pivotés conformément au calendrier de rotation. Secrets Manager calcule la date à laquelle la rotation doit avoir lieu. La règle est NON_COMPLIANT si la date est dépassée sans que la rotation n'ait été appliquée au secret.

> **Note**
>
> La règle renvoie NOT_APPLICABLE pour les secrets sans rotation.

Identificateur : SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

Types de ressources : AWS::SecretsManager::Secret

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

secretsmanager-secret-periodic-rotation

Vérifie si AWS les secrets de Secrets Manager ont fait l'objet d'une rotation au cours des derniers jours spécifiés. La règle est NON_COMPLIANT si un secret n'a pas fait l'objet d'une rotation pendant plus de jours que le nombre de jours de maxDaysSince rotation. La valeur par défaut est 90 jours.

Identificateur : SECRETSMANAGER_SECRET_PERIODIC_ROTATION

Types de ressources : AWS::SecretsManager::Secret

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

max DaysSinceRotation (facultatif), Type : int

Nombre maximum de jours pendant lesquels un secret peut rester inchangé. La valeur par défaut est 90 jours.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

secretsmanager-secret-unused

Vérifie si AWS les secrets de Secrets Manager ont été consultés dans un délai spécifié. La règle est NON_COMPLIANT si aucun secret n'a été consulté pendant un nombre de jours « non utilisés ForDays ». La valeur par défaut est 90 jours.

Contexte : il est recommandé de supprimer régulièrement les secrets inutilisés. Les secrets inutilisés peuvent être utilisés à mauvais escient par d'anciens utilisateurs qui n'ont plus besoin d'accéder à ces secrets. En outre, la probabilité que le secret soit utilisé à mauvais escient ou qu'un utilisateur accorde un accès à une entité non autorisée augmente à mesure qu'un nombre croissant d'utilisateurs accèdent à un secret. La suppression des secrets inutilisés permet de révoquer leur accès aux utilisateurs qui n'en ont plus besoin et de réduire les coûts d'utilisation AWS Secrets Manager.

Identificateur : SECRETSMANAGER_SECRET_UNUSED

Types de ressources : AWS::SecretsManager::Secret

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

unusedForDays (Facultatif), Type : int

Nombre de jours pendant lesquels un secret peut rester inchangé. La valeur par défaut est 90 jours.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

secretsmanager-using-cmk

Vérifie si tous les secrets AWS Secrets Manager sont chiffrés à l'aide de Clé gérée par AWS (`aws/secretsmanager`) ou d'une clé gérée par le client créée dans AWS Key Management Service (AWS KMS). La règle est COMPLIANT si un secret est chiffré à l'aide d'une clé gérée par le client. Cette règle est NON_COMPLIANT si un secret est chiffré à l'aide d'`aws/secretsmanager`.

> **Note**
>
> Cette règle n'a pas accès aux clés gérées par les clients entre comptes et renvoie NON_COMPLIANT pour les secrets qui utilisent une clé entre comptes.

Identificateur : SECRETSMANAGER_USING_CMK

Types de ressources : AWS::SecretsManager::Secret

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyArns (Facultatif), Type : CSV

Liste des Amazon Resource Names (ARN) de clés KMS séparés par des virgules, permettant de vérifier si les clés sont utilisées dans le chiffrement.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

securityhub-enabled

Vérifie si AWS Security Hub est activé pour un AWS compte. La règle est NON_COMPLIANT si AWS Security Hub n'est pas activé.

Identificateur : SECURITYHUB_ENABLED

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

security-account-information-provided

Vérifie si vous avez fourni les coordonnées de sécurité des contacts de votre AWS compte. La règle est NON_COMPLIANT si les informations de contact de sécurité du compte ne sont pas fournies.

Identificateur : SECURITY_ACCOUNT_INFORMATION_PROVIDED

Types de ressources : AWS::::Account

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

catalogue de services partagé au sein de l'organisation

Vérifie si AWS Service Catalog partage des portefeuilles avec une organisation (un ensemble de AWS comptes traités comme une seule unité) lorsque l'intégration avec AWS Organizations est activée. La règle est NON_COMPLIANT si la valeur « Type » d'une action est « ACCOUNT ».

Identifiant : SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

Types de ressources : AWS::ServiceCatalog::Portfolio

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

service-vpc-endpoint-enabled

Vérifie si un point de terminaison de service pour le service indiqué dans le paramètre de règle est créé pour chaque réseau Amazon Virtual Private Cloud (Amazon VPC). La règle renvoie NON_COMPLIANT si aucun point de terminaison d'un VPC n'est créé dans un réseau Amazon VPC pour le service.

Identificateur : SERVICE_VPC_ENDPOINT_ENABLED

Types de ressources : AWS : :EC2 : :VPC

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

serviceName, Type : chaîne

Nom abrégé ou suffixe du service. Remarque : Pour obtenir une liste des noms de service disponibles ou une liste de suffixes valides, utilisez DescribeVpcEndpointServices.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ses-malware-scanning-enabled

Vérifie si la recherche de programmes malveillants et de courrier indésirable est activée pour Amazon Simple Email Service (Amazon SES) lors de la réception de messages. La règle est NON_COMPLIANT si la recherche de programmes malveillants et de courrier indésirable n'est pas activée.

Identificateur : SES_MALWARE_SCANNING_ENABLED

Types de ressources : AWS::SES::ReceiptRule

Type de déclencheur : périodique

Région AWS : uniquement disponible dans les régions Europe (Irlande), USA Est (Virginie du Nord) et USA Ouest (Oregon)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

shield-advanced-enabled-autorenew

Vérifie si AWS Shield Advanced est activé sur votre AWS compte et si cet abonnement est configuré pour être renouvelé automatiquement. La règle est COMPLIANT si Shield Advanced et le renouvellement automatique sont activés.

> **Note**
>
> Le point de terminaison API de n' AWS Shield Advanced est disponible que dans la région USA Est (Virginie du Nord). Cette règle doit uniquement être planifiée pour s'exécuter dans la région USA Est (Virginie du Nord).

Identificateur : SHIELD_ADVANCED_ENABLED_AUTORENEW

Type de déclencheur : périodique

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

shield-drt-access

Vérifie si la Shield Response Team (SRT) peut accéder à votre AWS compte. La règle est NON_COMPLIANT si elle AWS Shield Advanced est activée mais que le rôle d'accès SRT n'est pas configuré.

Identificateur : SHIELD_DRT_ACCESS

Type de déclencheur : périodique

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sns-encrypted-kms

Vérifie si les sujets SNS sont chiffrés avec le service de gestion des AWS clés (AWS KMS). La règle est NON_COMPLIANT si un sujet SNS n'est pas chiffré avec KMS. AWS Spécifiez éventuellement les ARN clés, les ARN d'alias, le nom d'alias ou les ID de clé pour la règle à vérifier.

Identificateur : SNS_ENCRYPTED_KMS

Types de ressources : AWS::SNS::Topic

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

kmsKeyIds (Facultatif), Type : CSV

Liste séparée par des virgules des AWS noms de ressources Amazon (ARN), des ARN d'alias KMS, des noms d'alias KMS ou des identifiants de clé KMS à vérifier par la règle.

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

sns-topic-message-delivery-notification-enabled

Vérifie si la journalisation Amazon Simple Notification Service (SNS) est activée pour l'état de diffusion des messages de notification envoyés à une rubrique pour les points de terminaison. La règle est NON_COMPLIANT si la notification de l'état de diffusion des messages n'est pas activée.

Identificateur : SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

Types de ressources : AWS::SNS::Topic

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

ssm-document-not-public

Vérifie si AWS les documents Systems Manager détenus par le compte sont publics. La règle est NON_COMPLIANT si les documents Systems Manager détenus part le propriétaire « Self » sont publics.

Identificateur : SSM_DOCUMENT_NOT_PUBLIC

Types de ressources : AWS::SSM::Document

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

step-functions-state-machine-logging-enabled

Vérifie si la journalisation est activée sur la machine AWS Step Functions. La règle est NON_COMPLIANT si la journalisation n'est pas activée sur une machine d'état ou si la configuration de la journalisation ne respecte pas le niveau minimum indiqué.

Identificateur : STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

Types de ressources : AWS::StepFunctions::StateMachine

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

cloud WatchLogGroupArns (facultatif), Type : CSV

Liste séparée par des virgules des noms de ressources Amazon (ARN) pour les groupes de CloudWatch journaux Amazon Logs. La règle vérifie si les groupes de journaux spécifiés sont configurés pour les journaux de votre machine d'état.

logLevel (facultatif), Type : chaîne

Le niveau de journalisation minimum pour votre machine d'état. Les valeurs valides sont : ALL, ERROR, FATAL.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

storagegateway-last-backup-recovery-point-created

Vérifie si un point de restauration a été créé pour les volumes AWS Storage Gateway. La règle est NON_COMPLIANT si aucun point de récupération correspondant n'a été créé au cours de la période spécifiée dans le volume Storage Gateway.

Identificateur : STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::StorageGateway::Volume

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des volumes Storage Gateway pour la règle à vérifier, au format JSON `{"tagkey" : "tagValue"}`.

resourceId (facultatif), Type : chaîne

ID du volume Storage Gateway pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir Création de règles gérées AWS Config avec des modèles AWS CloudFormation.

storagegateway-resources-protected-by-backup-plan

Vérifie si les volumes AWS Storage Gateway sont protégés par un plan de sauvegarde. La règle est NON_COMPLIANT si aucun plan de sauvegarde n'est appliqué au volume Storage Gateway.

Identificateur : STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::StorageGateway::Volume

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Balises des volumes Storage Gateway pour la règle à vérifier, au format JSON.

resourceId (facultatif), Type : chaîne

ID du volume Storage Gateway pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

subnet-auto-assign-public-ip-disabled

Vérifie si une adresse IP publique est attribuée aux sous-réseaux Amazon Virtual Private Cloud (Amazon VPC). La règle est COMPLIANT si un réseau Amazon VPC ne présente aucun sous-réseau disposant d'une adresse IP publique. La règle est NON_COMPLIANT si une adresse IP publique est attribuée aux sous-réseaux d'un réseau Amazon VPC.

Identificateur : SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Types de ressources : AWS::EC2::Subnet

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

Évaluation proactive

Pour savoir comment exécuter cette règle en mode proactif, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour que cette règle renvoie COMPLIANT en mode proactif, le schéma de configuration des ressources de l'API StartResourced'évaluation doit inclure les entrées suivantes, codées sous forme de chaîne :

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

Pour plus d'informations sur l'évaluation proactive, consultez Mode d'évaluation.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

transfer-family-server-no-ftp

Vérifie si un serveur créé avec AWS Transfer Family utilise le protocole FTP pour la connexion des terminaux. La règle est NON_COMPLIANT si le protocole du serveur pour la connexion du point de terminaison est activé par FTP.

Identifiant : TRANSFER_FAMILY_SERVER_NO_FTP

Types de ressources : AWS::Transfer::Server

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

virtualmachine-last-backup-recovery-point-created

Vérifie si un point de restauration a été créé pour AWS Backup-Gateway VirtualMachines. La règle est NON_COMPLIANT si aucun point de restauration correspondant VirtualMachines n'a été créé dans le délai spécifié pour une AWS passerelle de sauvegarde.

Identificateur : VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

Types de ressources : AWS::BackupGateway::VirtualMachine

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Tags de AWS Backup-Gateway VirtualMachines pour la règle à vérifier, au format JSON. `{"tagkey" : "tagValue"}`

resourceId (facultatif), Type : chaîne

ID de AWS Backup-Gateway VirtualMachine pour la règle à vérifier.

récupération PointAgeValue (facultatif), Type : int, Valeur par défaut : 1

Valeur numérique pour l'âge maximum autorisé. Pas plus de 744 pour les heures et 31 pour les jours.

récupération PointAgeUnit (facultatif), Type : chaîne, Valeur par défaut : jours

Unité de temps correspondant à l'âge maximum autorisé. Valeurs acceptées : « heures », « jours ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation].

virtualmachine-resources-protected-by-backup-plan

Vérifie si AWS Backup-Gateway VirtualMachines est protégé par un plan de sauvegarde. La règle est NON_COMPLIANT si la passerelle de sauvegarde n' VirtualMachine est pas couverte par un plan de sauvegarde.

Identificateur : VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Types de ressources : AWS::BackupGateway::VirtualMachine

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

resourceTags (facultatif), Type : chaîne

Tags pour AWS Backup-Gateway VirtualMachines pour la règle à vérifier, au format JSON. `{"tagkey" : "tagValue"}`

resourceId (facultatif), Type : chaîne

ID de AWS Backup-Gateway VirtualMachine pour la règle à vérifier.

crossRegionList (Facultatif), Type : chaîne

Liste des régions de destination séparées par des virgules pour la copie de sauvegarde interrégionale à conserver

crossAccountList (Facultatif), Type : chaîne

Liste des comptes de destination séparés par des virgules pour la copie de sauvegarde entre comptes à conserver

maxRetentionDays (Facultatif), Type : int

Période de conservation maximale exprimée en jours pour le Backup Vault Lock

minRetentionDays (Facultatif), Type : int

Période de conservation minimale exprimée en jours pour le Backup Vault Lock

sauvegarde VaultLockCheck (facultatif), Type : chaîne

Valeurs acceptées : « True » ou « False ». Saisissez « True » pour la règle afin de vérifier si la ressource est sauvegardée dans un coffre verrouillé

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

vpc-default-security-group-closed

Vérifie si le groupe de sécurité par défaut d'un réseau Amazon Virtual Private Cloud (Amazon VPC) n'autorise pas le trafic entrant ou sortant. La règle est NON_COMPLIANT si le groupe de sécurité par défaut comporte une ou plusieurs règles de trafic entrant ou sortant.

> **Note**
>
> Il peut y avoir un délai entre les AWS Config enregistrements de la suppression des ressources associées, telles que les groupes de sécurité par défaut, qui sont supprimés dans le cadre de la suppression d'Amazon VPC. Par conséquent, même si tous les groupes de sécurité par défaut ou d'autres ressources associées ont été supprimés ou corrigés, la règle peut indiquer NON_COMPLIANT jusqu'au prochain processus de référence du compte.

Identificateur : VPC_DEFAULT_SECURITY_GROUP_CLOSED

Types de ressources : AWS::EC2::SecurityGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

vpc-flow-logs-enabled

Vérifie si les journaux de flux Amazon Virtual Private Cloud (Amazon VPC) sont activés et figurent dans l'ensemble des réseaux Amazon VPC. La règle est NON_COMPLIANT si les journaux de flux ne sont pas activés dans au moins un réseau Amazon VPC.

Identificateur : VPC_FLOW_LOGS_ENABLED

Types de ressources : AWS : :EC2 : :VPC

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

trafficType (facultatif), Type : chaîne

TrafficType de journaux de flux

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

vpc-network-acl-unused-check

Vérifie si certaines listes de contrôle d'accès au réseau (ACL réseau) sont inutilisées. La règle est COMPLIANT si chaque liste ACL réseau est associée à un sous-réseau. La règle est NON_COMPLIANT si aucune liste ACL réseau n'est associée à un sous-réseau.

Identificateur : VPC_NETWORK_ACL_UNUSED_CHECK

Types de ressources : AWS::EC2::NetworkAcl

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

vpc-peering-dns-resolution-check

Vérifie si la résolution DNS d'un réseau VPC accepteur/demandeur est activée vers une adresse IP privée. La règle est NON_COMPLIANT si la résolution DNS d'un réseau VPC accepteur/demandeur n'est pas activée vers une adresse IP privée.

Identificateur : VPC_PEERING_DNS_RESOLUTION_CHECK

Types de ressources : AWS : :EC2 : :VPC PeeringConnection

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

vpcIds (facultatif), Type : CSV

Liste des ID de réseaux VPC à vérifier, séparés par des virgules.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

vpc-sg-open-only-to-authorized-ports

Vérifie si les groupes de sécurité autorisant le trafic entrant illimité (« 0.0.0.0/0 » ou « ::/0 ») n'autorisent que les connexions TCP ou UDP entrantes sur les ports autorisés. La règle est NON_COMPLIANT si les ports de ces groupes de sécurité ne sont pas spécifiés dans les paramètres de la règle.

> **Note**
>
> Cette règle évalue les groupes de sécurité Amazon EC2 dont la règle de trafic entrant est définie sur IPv4=« 0.0.0.0/0 » or IPv6=« ::/ ». Si le groupe de sécurité ne présente aucune de ces destinations, cette règle renvoie `NOT_APPLICABLE`.

Identificateur : VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

Types de ressources : AWS::EC2::SecurityGroup

Type de déclencheur : modifications de configuration et périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

authorizedTcpPorts (Facultatif), Type : chaîne

Liste des ports TCP autorisés à être ouverts sur 0.0.0.0/0 ou ::/0, séparés par des virgules. Les plages sont définies par des tirets, par exemple « 443,1020-1025 ».

authorizedUdpPorts (Facultatif), Type : chaîne

Liste des ports UDP autorisés à être ouverts sur 0.0.0.0/0 ou ::/0, séparés par des virgules. Les plages sont définies par des tirets, par exemple, « 500 1020-1025 ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

contrôle des restrictions de port vpc-sg-

Vérifie si les groupes de sécurité limitent explicitement le trafic entrant aux ports restreints à partir de 0.0.0.0/0 ou : :/0. La règle est NON_COMPLIANT si les groupes de sécurité autorisent le trafic entrant depuis 0.0.0.0/0 ou : :/0 via les ports TCP/UDP 22/3389 ou comme indiqué dans les paramètres.

Identifiant : VPC_SG_PORT_RESTRICTION_CHECK

Types de ressources : AWS::EC2::SecurityGroup

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

RestrictPorts (facultatif), Type : CSV

Liste séparée par des virgules des ports qui ne doivent pas être ouverts au trafic entrant sur toute la plage d'adresses IP. Les numéros de port valides sont compris entre 0 et 65535. Si elle n'est pas spécifiée, la règle vérifie par défaut 22 et 3389.

Type de protocole (facultatif), Type : chaîne

Type de protocole de transmission pour la règle à vérifier. Les valeurs valides incluent « TCP », « UDP » et « ALL » (sans distinction majuscules/majuscules). Si elle est définie sur « ALL », la

règle vérifiera les règles qui utilisent le protocole « TCP », « UDP » ou « ALL » (-1). La valeur par défaut est « TOUS ».

exclure ExternalSecurityGroups (facultatif), Type : valeur booléenne

Indicateur booléen pour exclure l'évaluation des groupes de sécurité externes. Si elle est définie sur « true », la règle n'inclura pas les groupes de sécurité externes dans l'évaluation. Sinon, tous les groupes de sécurité sont évalués si la valeur est définie sur « faux ». La valeur par défaut est « true ».

Type IP (facultatif), Type : chaîne

Version du protocole Internet (IP) de la règle à vérifier. Les valeurs valides incluent « IPv4 », « IPv6 » et « ALL » (sans distinction majuscules/minuscules). Si elle n'est pas spécifiée, la règle vérifie par défaut « TOUT ».

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

vpc-vpn-2-tunnels-up

Vérifie si les deux tunnels de réseau privé virtuel (VPN) fournis par le AWS VPN Site-to-site sont en état UP. La règle est NON_COMPLIANT si l'un des tunnels ou les deux présentent l'état DOWN.

Identificateur : VPC_VPN_2_TUNNELS_UP

Types de ressources : AWS::EC2::VPNConnection

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

wafv2-logging-enabled

Vérifie si la journalisation est activée sur les listes de contrôle d'accès Web (ACL Web) régionales et mondiales du AWS WAFv2. La règle est NON_COMPLIANT si la journalisation est activée sans que la destination de journalisation ne corresponde à la valeur du paramètre.

Identificateur : WAFV2_LOGGING_ENABLED

Types de ressources : AWS::WAFv2::Web ACL

Type de déclencheur : périodique

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

KinesisFirehoseDeliveryStreamArns (Facultatif), Type : CSV

La liste des ARN de flux de diffusion Kinesis Firehose, séparés par des virgules

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voir[Création de règles gérées AWS Config avec des modèles AWS CloudFormation](#).

wafv2-rulegroup-logging-enabled

Vérifie si la collecte des métriques CloudWatch de sécurité Amazon sur les groupes de règles AWS WAFv2 est activée. La règle est NON_COMPLIANT si le paramètre '. VisibilityConfig CloudWatchMetricsEnabledle champ 'est défini sur false.

Contexte : AWS WAFV2 (Web Application Firewall version 2) vous permet de créer des AWS WAF règles pour protéger vos applications Web contre les vulnérabilités et les exploits Web courants. Un groupe de AWS WAF règles est un ensemble de AWS WAF règles que vous pouvez associer à une liste de contrôle d'accès (ACL) Web afin de définir le comportement souhaité pour le trafic de votre application Web. Pour plus d'informations, consultez [AWS WAF les règles et les](#) [groupes de règles](#) dans le guide du AWS WAF développeur.

En configurant la collecte de mesures de CloudWatch sécurité sur un groupe de AWS WAFV2 règles, vous pouvez surveiller les mesures de sécurité telles que la réussite ou l'échec des attaques par déni

de service distribué (DDoS), l'injection SQL et les attaques par script intersite (XSS). Les indicateurs de sécurité collectés peuvent vous aider à simplifier vos enquêtes.

> **Note**
>
> Si le groupe de AWS WAF règles ne contient aucune AWS WAFV2 règle à vérifier AWS Config par la règle gérée, celle-ci AWS Config renvoie NON_APPLICABLE.

Identificateur : WAFV2_RULEGROUP_LOGGING_ENABLED

Types de ressources : AWS::WAFv2::RuleGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

wafv2-rulegroup-not-empty

Vérifie si les groupes de règles WAFv2 contiennent des règles. La règle est NON_COMPLIANT si aucune règle ne figure dans un groupe de règles WAFv2.

Identificateur : WAFV2_RULEGROUP_NOT_EMPTY

Types de ressources : AWS::WAFv2::RuleGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

wafv2-webacl-not-empty

Vérifie si une liste ACL Web WAFv2 contient des règles ou des groupes de règles WAF. Cette règle est NON_COMPLIANT si une liste ACL Web ne contient aucune règle ou aucun groupe de règles WAF.

Identificateur : WAFV2_WEBACL_NOT_EMPTY

Types de ressources : AWS::WAFv2::Web ACL

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

waf-classic-logging-enabled

Vérifie si la journalisation est activée sur les listes de contrôle d'accès Web globales (ACL Web) AWS WAF Classic. La règle est NON_COMPLIANT si la journalisation n'est pas activée sur une liste ACL Web.

Identificateur : WAF_CLASSIC_LOGGING_ENABLED

Types de ressources : AWS::WAF::Web ACL

Type de déclencheur : périodique

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

KinesisFirehoseDeliveryStreamArns (Facultatif), Type : CSV

Liste séparée par des virgules de l'ARN des flux Amazon Kinesis AWS pour les journaux WAF.

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

waf-global-rulegroup-not-empty

Vérifie si un groupe de règles AWS WAF Classic contient des règles. La règle est NON_COMPLIANT si aucune règle ne figure dans un groupe de règles.

Identificateur : WAF_GLOBAL_RULEGROUP_NOT_EMPTY

Types de ressources : AWS::WAF::RuleGroup

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

waf-global-rule-not-empty

Vérifie si une règle globale AWS WAF contient des conditions. La règle est NON_COMPLIANT si aucune condition ne figure dans la règle globale WAF.

Identificateur : WAF_GLOBAL_RULE_NOT_EMPTY

Types de ressources : AWS::WAF::Rule

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

waf-global-webacl-not-empty

Vérifie si une liste ACL Web Global WAF contient des règles ou des groupes de règles WAF. Cette règle est NON_COMPLIANT si une liste ACL Web ne contient aucune règle ou aucun groupe de règles WAF.

Identificateur : WAF_GLOBAL_WEBACL_NOT_EMPTY

Types de ressources : AWS::WAF::Web ACL

Type de déclencheur : changements de configuration

Région AWS : uniquement disponible dans la région USA Est (Virginie du Nord)

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

waf-regional-rulegroup-not-empty

Vérifie si les groupes de règles WAF Regional contiennent des règles. La règle est NON_COMPLIANT si aucune règle ne figure dans un groupe de règles WAF Regional.

Identificateur : WAF_REGIONAL_RULEGROUP_NOT_EMPTY

Types de ressources : AWS::WAFRegional::RuleGroup

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

waf-regional-rule-not-empty

Vérifie si la règle régionale WAF contient des conditions. Cette règle est COMPLIANT si la règle régionale contient au moins une condition. Elle est NON_COMPLIANT dans le cas contraire.

Identificateur : WAF_REGIONAL_RULE_NOT_EMPTY

Types de ressources : AWS::WAFRegional::Rule

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

waf-regional-webacl-not-empty

Vérifie si une liste ACL Web WAF régionale contient des règles ou des groupes de règles WAF. La règle est NON_COMPLIANT si aucune règle ou aucun groupe de règles WAF ne figure dans une liste ACL Web.

Identificateur : WAF_REGIONAL_WEBACL_NOT_EMPTY

Types de ressources : AWS::WAFRegional::Web ACL

Type de déclencheur : changements de configuration

Région AWS: Toutes les AWS régions prises en charge

Paramètres :

Aucun

AWS CloudFormation modèle

Pour créer des règles AWS Config gérées à l'aide AWS CloudFormation de modèles, voirCréation de règles gérées AWS Config avec des modèles AWS CloudFormation.

Liste des règles AWS Config gérées par mode d'évaluation

AWS Config prend actuellement en charge les règles gérées suivantes.

Considérations

Valeurs par défaut pour les règles gérées

Les valeurs par défaut spécifiées pour les règles gérées sont préremplies uniquement lors de l'utilisation de la AWS console. Les valeurs par défaut ne sont pas fournies pour l'API, la CLI ou le kit SDK.

Les compartiments de répertoire ne sont pas pris en charge

Les règles gérées ne prennent en charge que les compartiments à usage général lors de l'évaluation des ressources Amazon Simple Storage Service (Amazon S3). AWS Config n'enregistre pas les modifications de configuration pour les compartiments de répertoire. Pour plus d'informations sur les compartiments à usage général et les compartiments de répertoires, consultez Présentation des compartiments et Compartiments de répertoires dans le Guide de l'utilisateur Amazon S3.

Règles gérées et types de ressources IAM globaux

Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS

Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Évaluation proactive

Les règles proactives sont des règles qui prennent en charge le mode d'évaluation proactive pour les ressources qui n'ont pas été déployées. Cela vous permet d'évaluer si un ensemble de propriétés de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région. Pour plus d'informations, consultez Modes d'évaluation.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Évaluation proactive

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-public-access-check
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled

Évaluation détective

Les règles détectives sont des règles qui prennent en charge le mode d'évaluation détective pour les ressources déjà déployées. Ce type d'évaluation vous permet d'évaluer les paramètres de configuration de vos ressources existantes.

> **Note**
>
> À l'heure actuelle, toutes les AWS Config règles soutiennent l'évaluation des détectives.

Évaluation détective

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging

- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user

- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda

- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-s3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- vérification de l'expiration du certificat du serveur iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Liste des règles AWS Config gérées par type de déclencheur

AWS Config prend actuellement en charge les règles gérées suivantes.

Considérations

Valeurs par défaut pour les règles gérées

Les valeurs par défaut spécifiées pour les règles gérées sont préremplies uniquement lors de l'utilisation de la AWS console. Les valeurs par défaut ne sont pas fournies pour l'API, la CLI ou le kit SDK.

Les compartiments de répertoire ne sont pas pris en charge

Les règles gérées ne prennent en charge que les compartiments à usage général lors de l'évaluation des ressources Amazon Simple Storage Service (Amazon S3). AWS Config n'enregistre pas les modifications de configuration pour les compartiments de répertoire. Pour plus d'informations sur les compartiments à usage général et les compartiments de répertoires, consultez Présentation des compartiments et Compartiments de répertoires dans le Guide de l'utilisateur Amazon S3.

Règles gérées et types de ressources IAM globaux

Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS

Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge. Pour obtenir la liste des règles gérées prises en charge dans quelles régions, consultez la section Liste des règles AWS Config gérées par disponibilité des régions.

Changements de configuration

Les règles déclenchées par des modifications sont des règles qui sont AWS Config évaluées en réponse aux modifications de configuration.

Changements de configuration

- acm-certificate-rsa-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest

- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled

- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-client-vpn-connection-log-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- global-endpoint-event-replication-enabled

- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- catalogue de services partagé au sein de l'organisation
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Périodique

Les règles périodiques sont des règles qui AWS Config sont évaluées périodiquement à une fréquence que vous spécifiez, par exemple toutes les 24 heures.

Périodique

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance

- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-s3 activée
- compatible avec l'analyseur d'accès externe iam
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- vérification de l'expiration du certificat du serveur iam
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- Kinesis-Firehose Delivery Stream crypté
- kms-cmk-not-scheduled-for-deletion
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled

- netfw-logging-enabled
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-resources-protected-by-backup-plan
- accès au port non restreint par redshift
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan

- vpc-flow-logs-enabled
- contrôle des restrictions de port vpc-sg-
- wafv2-logging-enabled
- waf-classic-logging-enabled

Hybride

Les règles hybrides sont des règles qui AWS Config évaluent à la fois en réponse aux modifications de configuration et périodiquement.

Hybride

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- incoming-ssh-disabled
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

Liste des règles AWS Config gérées par région et disponibilité

AWS Config prend actuellement en charge les règles gérées suivantes.

Considérations

Valeurs par défaut pour les règles gérées

Les valeurs par défaut spécifiées pour les règles gérées sont préremplies uniquement lors de l'utilisation de la AWS console. Les valeurs par défaut ne sont pas fournies pour l'API, la CLI ou le kit SDK.

Les compartiments de répertoire ne sont pas pris en charge

Les règles gérées ne prennent en charge que les compartiments à usage général lors de l'évaluation des ressources Amazon Simple Storage Service (Amazon S3). AWS Config n'enregistre pas les

modifications de configuration pour les compartiments de répertoire. Pour plus d'informations sur les compartiments à usage général et les compartiments de répertoires, consultez Présentation des compartiments et Compartiments de répertoires dans le Guide de l'utilisateur Amazon S3.

Règles gérées et types de ressources IAM globaux

Les types de ressources IAM globaux intégrés avant février 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy``AWS::IAM::Role`, et`AWS::IAM::User`) ne peuvent être enregistrés que AWS Config dans les AWS régions où ils AWS Config étaient disponibles avant février 2022. Ces types de ressources ne peuvent pas être enregistrés dans les régions prises en charge AWS Config après février 2022. Pour une liste de ces régions, voir AWS Ressources d'enregistrement | Ressources mondiales.

Si vous enregistrez un type de ressource IAM global dans au moins une région, les règles périodiques qui indiquent la conformité au type de ressource IAM global exécuteront des évaluations dans toutes les régions où la règle périodique est ajoutée, même si vous n'avez pas activé l'enregistrement du type de ressource IAM global dans la région où la règle périodique a été ajoutée.

Pour éviter des évaluations inutiles, vous devez uniquement déployer des règles périodiques qui signalent la conformité d'un type de ressource IAM global à l'une des régions prises en charge.

Région US East (Ohio)

USA Est (Ohio)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check

- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance

- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check

- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région USA Est (Virginie du Nord)

USA Est (Virginie du Nord)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging

- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user

- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda

- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- vérification de l'expiration du certificat du serveur iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery Stream crypté
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région US West (N. California)

USA Ouest (Californie du Nord)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check

- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit

- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication

- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région USA Ouest (Oregon)

USA Ouest (Oregon)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée

- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Afrique (Le Cap)

Afrique (Le Cap)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan

- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- compatible DMS-REDIS-TLS
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé

- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check

- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance

- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asie-Pacifique (Hong Kong)

Asie-Pacifique (Hong Kong)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest

- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled

- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled

- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asie-Pacifique (Hyderabad)

Asie-Pacifique (Hyderabad)

- acm-certificate-expiration-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-accessible au public
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- protection guardduty-S3 activée
- compatible avec l'analyseur d'accès externe iam
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- Kinesis-Firehose Delivery-Stream crypté
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-default-admin-check
- redshift-default-db-name-check
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Région Asie-Pacifique (Jakarta)

Asie-Pacifique (Jakarta)

- access-keys-rotated

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-multiple-az
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-accessible au public
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- Kinesis-Firehose Delivery-Stream crypté
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-default-admin-check
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public

- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

Région Asie-Pacifique (Melbourne)

Asie-Pacifique (Melbourne)

- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs-mount-target-accessible au public
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- protection guardduty-S3 activée
- compatible avec l'analyseur d'accès externe iam
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asie-Pacifique (Mumbai)

Asie-Pacifique (Mumbai)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check

- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check

- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups

- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled

- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asie-Pacifique (Osaka)

Asie-Pacifique (Osaka)

- access-keys-rotated
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-launch-template-public-ip-disabled
- ec2-no-amazon-key-pair
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecs-containers-readonly-access
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-mount-target-accessible au public
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elbv2-multiple-az
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-no-statements-with-admin-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-function-public-access-prohibited
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-cluster-default-admin-check
- rds-cluster-encrypted-at-rest
- rds-instance-default-admin-check
- rds-instance-public-access-check
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public

- step-functions-state-machine-logging-enabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-peering-dns-resolution-check
- contrôle des restrictions de port vpc-sg-
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asia Pacific (Seoul)

Asie-Pacifique (Séoul)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check

- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check

- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable

- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports

- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asie-Pacifique (Singapour)

Asie-Pacifique (Singapour)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id

- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail

- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan

- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target

- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asie-Pacifique (Sydney)

Asie-Pacifique (Sydney)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check

- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled

- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check

- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted

- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check

- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check

- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check

- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created

- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Asie-Pacifique (Tokyo)

Asie-Pacifique (Tokyo)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check

- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created

- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Canada (Centre)

Canada (Centre)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- Cloudtrail-all-write-s3-data-event-check
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check

- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check

- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check

- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Canada Ouest (Calgary)

Canada Ouest (Calgary)

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- approved-amis-by-id
- approved-amis-by-tag
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- eip-attached
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Région Chine (Beijing)

Chine (Beijing)

- access-keys-rotated

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- journalisation de l'accès à un compartiment à 3 compartiments avec Cloudtrail

- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Chine (Ningxia)

Chine (Ningxia)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3

- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled

- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

Région Europe (Francfort)

Europe (Francfort)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé

- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Europe (Irlande)

Europe (Irlande)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée

- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- compatible avec la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Europe (Londres)

Europe (Londres)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag

- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan

- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift-unrestricted-
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Europe (Milan) Region

Europe (Milan)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- compatible DMS-REDIS-TLS
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted

- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- accès au port non restreint par redshift-unrestricted-

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Europe (Paris)

Europe (Paris)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized

- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Europe (Espagne)

Europe (Espagne)

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-accessible au public
- eip-attached
- eks-cluster-log-enabled

- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- protection guardduty-S3 activée
- compatible avec l'analyseur d'accès externe iam
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- Kinesis-Firehose Delivery-Stream crypté
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- rds-instance-default-admin-check
- redshift-default-admin-check
- redshift-default-db-name-check
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ssm-document-not-public

- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Région Europe (Stockholm)

Europe (Stockholm)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id

- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required

- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée

- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- compatible avec le scan de code inspector-lambda
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région Europe (Zurich)

Europe (Zurich)

- account-part-of-organizations

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-accessible au public
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- elb-deletion-protection-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé

- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- protection guardduty-S3 activée
- compatible avec l'analyseur d'accès externe iam
- iam-password-policy
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-snapshot-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Région Israël (Tel Aviv)

Israël (Tel Aviv)

- account-part-of-organizations

- alb-desync-mode-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- eip-attached
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- protection guardduty-S3 activée
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- contrôle des restrictions de port vpc-sg-
- wafv2-webacl-not-empty

Middle East (Bahrain) Region

Moyen-Orient (Bahreïn)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection

- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public

- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Région du Moyen-Orient (EAU)

Moyen-Orient (EAU)

- account-part-of-organizations
- acm-certificate-expiration-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs-mount-target-accessible au public
- eks-cluster-log-enabled

- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- protection guardduty-S3 activée

- compatible avec l'analyseur d'accès externe iam
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-rabbit-deployment-mode
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled

- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Région Amérique du Sud (São Paulo)

Amérique du Sud (São Paulo)

- access-keys-rotated
- account-part-of-organizations

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- chiffrement des points de terminaison dax-tls
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit activé
- guardduty-eks-protection-runtime activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- activé par guardduty-malware-protection
- guardduty-non-archived-findings
- guardduty-rds-protection activé
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- compatible avec l'analyseur d'accès externe iam

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- vérification automatique de la découverte des données Macie-Auto-Sensitive

- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- compatible avec mq-cloudwatch-audit-log
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

AWS GovCloud Région (USA Est)

AWS GovCloud (USA Est)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée
- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-resources-protected-by-backup-plan
- guardduty-eks-protection-audit activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- guardduty-non-archived-findings
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- compatible avec mq-cloudwatch-audit-log
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- catalogue de services partagé au sein de l'organisation
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud Région (US-Ouest)

AWS GovCloud (US-Ouest)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- Cloudtrail-all-read-s3-data-event-check
- vérification des événements de données cloudtrail-all-write-s3
- journalisation des accès au compartiment 3 dans le cloud trail
- accès public à cloudtrail-s3-bucket interdit
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- Authentification DMS-MONGO-DB activée
- Autorisation DMS-NEPTUNE-IAM activée

- compatible DMS-REDIS-TLS
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-accessible au public
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-resources-protected-by-backup-plan
- guardduty-eks-protection-audit activé
- guardduty-enabled-centralized
- compatible avec la protection GuardDuty-Lambda
- guardduty-non-archived-findings
- protection guardduty-S3 activée
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- vérification de l'expiration du certificat du serveur iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- compatible avec inspector-ec2-scan
- compatible avec inspector-ecr-scan
- inspector-lambda compatible avec le scan standard
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- Kinesis-Firehose Delivery-Stream crypté
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- compatible avec mq-cloudwatch-audit-log
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- accès au port non restreint par redshift
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- Activé pour la réplication entre régions du compartiment S3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- catalogue de services partagé au sein de l'organisation

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- contrôle des restrictions de port vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Règles liées aux services AWS Config

Une AWS Config règle liée à un service est un type unique de règles AWS Config gérées qui permet à d'autres AWS services de créer des AWS Config règles dans votre compte. Les règles liées aux services sont prédéfinies pour inclure toutes les autorisations requises pour appeler d'autres AWS services en votre nom. Ces règles sont similaires aux normes qu'un AWS service vous recommande Compte AWS pour la vérification de conformité.

Ces AWS Config règles liées aux services sont détenues par les équipes de AWS service. L'équipe AWS de service crée ces règles dans votre Compte AWS. Vous disposez d'un accès en lecture seule à ces règles. Vous ne pouvez pas modifier ou supprimer ces règles si vous êtes abonné à AWS un service auquel ces règles sont liées.

Les règles liées aux services et le AWS Command Line Interface

Lorsque les AWS CLI API PutConfigRule, DeleteConfigRule et DeleteEvaluationResults renvoient l'accès refusé avec le message d'erreur suivant :

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

Les règles liées aux services et la console AWS Config

Dans la AWS Config console, les AWS Config règles liées au service sont visibles sur la page Règles. Les boutons Modifier et Supprimer les résultats sont grisés dans la console pour vous empêcher de modifier la règle. Vous pouvez consulter les détails de la règle en choisissant celle-ci.

Règles liées aux services, actions correctives et packs de conformité

Pour ajouter des actions de correction à des règles liées à un service dans un pack de conformité, vous devez ajouter l'action de correction au modèle de pack de conformité lui-même, puis mettre à jour le pack de conformité avec votre modèle mis à jour. Pour plus d'informations sur la mise à jour des packs de conformité, consultez les sections Déploiement d'un pack de conformité (console), Déploiement d'un pack de conformité (AWS CLI) et Gestion des packs de conformité organisationnels.

Modification et suppression de règles liées à un service

Pour modifier ou supprimer une règle liée à un service, contactez le AWS service qui a créé la règle. Par exemple, pour les règles liées à un service créées par AWS Security Hub, vous pouvez supprimer une règle liée à un service en suivant les étapes décrites dans le Guide de l'AWS Security Hub utilisateur : Désactivation d'une norme de sécurité.

Création de règles gérées AWS Config avec des modèles AWS CloudFormation

> **Important**
>
> Vous devez d'abord créer et démarrer l'enregistreur deAWS Config configuration afin de créer des règlesAWS Config gérées avecAWS CloudFormation. Pour de plus amples informations, veuillez consulter Gestion de l'enregistreur de configuration.

Pour les règles gérées AWS Config prises en charge, vous pouvez utiliser les modèles AWS CloudFormation pour créer la règle pour votre compte ou mettre à jour une pile AWS CloudFormation existante. Une pile est un ensemble de ressources associées que vous mettez en service et à jour en tant qu'unité unique. Lorsque vous lancez une pile avec un modèle, la règle gérée AWS Config

est créée pour vous. Les modèles créent uniquement la règle et ne créent pas de ressources AWS supplémentaires.

> **Note**
>
> Lorsque les règles gérées AWS Config sont mises à jour, les modèles sont mis à jour pour les dernières modifications. Pour enregistrer une version spécifique d'un modèle pour une règle, téléchargez le modèle et chargez-le dans votre compartiment S3.

Pour plus d'informations sur l'utilisation desAWS CloudFormation modèles, consultez la section MiseAWS CloudFormation en route du Guide deAWS CloudFormation l'utilisateur.

Pour lancer une pile AWS CloudFormation pour une règle gérée AWS Config

1. Accédez à la CloudFormationconsole et créez une nouvelle pile.
2. Pour Specify template (Spécifier un modèle) :
   - Si vous avez téléchargé le modèle, choisissez Upload a template file (Charger un fichier de modèle), puis choisissez Choose file (Choisir un fichier) pour charger le modèle.
   - Vous pouvez également choisir l'URL Amazon S3 et saisir l'URL du modèle`http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/`*`THE_RULE_IDENTIFIER`*`.template`.

   > **Note**
   >
   > L'identifiant de la règle doit être écrit dans ALL_CAPS_WITH_UNDERSCORES. Par exemple, CLOUDWATCH_LOG_GROUP_ENCRYPTED au lieu decloudwatch-log-group-encrypted.
   > Pour certaines règles, l'identifiant de la règle est différent du nom de la règle. Assurez-vous d'utiliser l'option d'utilisation. Par exemple, l'identifiant de règle pour restricted-ssh est INCOMING_SSH_DISABLED.

3. Choisissez Next (Suivant).
4. Pour Specify stack details (Spécifier les détails de pile), entrez un nom de pile et des valeurs de paramètre pour la règle AWS Config. Par exemple, si vous utilisez le modèle de règle gérée `DESIRED_INSTANCE_TYPE`, vous pouvez spécifier le type d'instance comme « m4.large ».

5. Choisissez Next (Suivant).
6. Pour Options, vous pouvez créer des balises ou configurer d'autres options avancées. Celles-ci ne sont pas obligatoires.
7. Choisissez Next (Suivant).
8. Pour Vérifier, vérifiez que le modèle, les paramètres et les autres options sont corrects.
9. Sélectionnez Create (Créer). La pile est créée en quelques minutes. Vous pouvez afficher la règle créée dans la console AWS Config.

Vous pouvez utiliser les modèles pour créer une pile unique pour les règles gérées AWS Config ou mettre à jour une pile existante dans votre compte. Si vous supprimez une pile, les règles gérées créées à partir de cette pile sont également supprimées. Pour plus d'informations, consultez la section Utilisation des piles dans le guide deAWS CloudFormation l'utilisateur.

AWS Config Règles personnalisées

AWS Config Les règles personnalisées sont des règles que vous créez de toutes pièces. Il existe deux manières de créer des règles AWS Config personnalisées : avec les fonctions Lambda (Guide du AWS Lambda développeur) et avec Guard (Guard GitHub Repository), un policy-as-code langage.

AWS Config les règles personnalisées créées avec Lambda sont appelées règles AWS Config Lambda AWS Config personnalisées et les règles personnalisées créées avec Guard sont appelées AWS Config règles de politique personnalisées.

AWS Config Règles de politique personnalisées

Les règles écrites à l'aide de Guard peuvent être créées à partir de la AWS Config console ou à l'aide des API de AWS Config règles. AWS Config Les règles de politique personnalisées vous permettent de créer des règles AWS Config personnalisées sans avoir à utiliser Java ou Python pour développer des fonctions Lambda afin de gérer vos règles personnalisées. AWS Config Les règles de politique personnalisées sont initiées par des modifications de configuration. Pour plus d'informations sur Guard, consultez le GitHubréférentiel Guard.

AWS Config Règles Lambda personnalisées

Les règles Lambda personnalisées vous permettent d'utiliser Java ou Python pour créer une fonction Lambda pour une règle personnalisée. AWS Config Une fonction Lambda est un code personnalisé que vous téléchargez et qui est invoqué par des événements qui y sont publiés par une source

d'événements. AWS Lambda Si la fonction Lambda est associée à une AWS Config règle, elle l' AWS Config invoque lorsque la règle est initiée. La fonction Lambda évalue ensuite les informations de configuration envoyées par et renvoie AWS Config les résultats de l'évaluation. Pour plus d'informations sur les fonctions Lambda, consultez Fonction et sources d'événements dans le Guide du développeur AWS Lambda .

Considérations de coût

Pour plus de détails sur les coûts associés à l'enregistrement des ressources, consultez la section AWS Config tarification.

Recommandation : ajouter une logique pour gérer l'évaluation des ressources supprimées pour les règles Lambda personnalisées

Lorsque vous créez AWS Config des règles lambda personnalisées, il est vivement recommandé d'ajouter une logique pour gérer l'évaluation des ressources supprimées.

Lorsque les résultats de l'évaluation sont marqués comme `NOT_APPLICABLE`, ils seront marqués pour suppression et nettoyés. S'ils ne sont PAS marqués comme `NOT_APPLICABLE`, les résultats de l'évaluation resteront inchangés jusqu'à ce que la règle soit supprimée, en risquant d'entraîner une augmentation inattendue de la création d'éléments de configuration (CI) pour `AWS::Config::ResourceCompliance` lors de la suppression de la règle.

Pour plus d'informations sur la façon de définir AWS Config des règles Lambda personnalisées `NOT_APPLICABLE` pour récupérer les ressources supprimées, voir Gestion des ressources supprimées à l'aide de règles Lambda AWS Config personnalisées.

Recommandation : fournir les ressources nécessaires pour les règles Lambda personnalisées

AWS Config Les règles Lambda personnalisées peuvent entraîner un nombre élevé d'appels de fonctions Lambda si la règle n'est pas limitée à un ou plusieurs types de ressources. Pour éviter une augmentation de l'activité associée à votre compte, il est vivement recommandé de fournir des ressources correspondant à vos règles Lambda personnalisées. Si aucun type de ressource n'est sélectionné, la règle invoquera la fonction Lambda pour toutes les ressources du compte.

Recommandation : arrêtez d'enregistrer la conformité des ressources avant de supprimer les règles

Il est vivement recommandé d'arrêter l'enregistrement pour le type de `AWS::Config::ResourceCompliance` ressource avant de supprimer les règles de votre compte. La suppression de règles crée des CI pour votre enregistreur de AWS Config configuration

`AWS::Config::ResourceCompliance` et peut avoir une incidence sur les coûts de votre enregistreur. Si vous supprimez des règles qui évaluent un grand nombre de types de ressources, cela peut entraîner une augmentation du nombre de CI enregistrés.

Bonnes pratiques :

1. Arrêter l'enregistrement `AWS::Config::ResourceCompliance`
2. Supprimer une ou plusieurs règles
3. Activez l'enregistrement pour `AWS::Config::ResourceCompliance`

Types de déclencheurs

Après avoir ajouté une règle à votre compte, AWS Config comparez vos ressources aux conditions de cette règle. Après cette évaluation initiale, AWS Config continue à exécuter des évaluations chaque fois qu'une évaluation est déclenchée. Les déclencheurs d'évaluation sont définis dans le cadre de la règle et peuvent inclure les types suivants.

Type de déclencheur	Description
Configuration changes	AWS Config exécute des évaluations pour la règle lorsqu'une ressource correspond au champ d'application de la règle et qu'il y a un changement de configuration de la ressource. L'évaluation s'exécute après l' AWS Config envoi d'une notification de modification d'élément de configuration. Vous choisissez quelles ressources déclenche nt l'évaluation en définissant la portée de la règle. La portée peut inclure les éléments suivants : • Un ou plusieurs types de ressources • Une combinaison d'un type de ressource et d'un ID de ressource • Une combinaison d'une clé de balise et d'une valeur

Type de déclencheur	Description
	• Lorsqu'une ressource enregistrée est créée, mise à jour ou supprimée AWS Config exécute l'évaluation lorsqu'il détecte une modification apportée à une ressource correspondant au champ d'applica tion de la règle. Vous pouvez utiliser la portée afin de définir les ressources qui déclenchent des évaluations.
Périodique	AWS Config exécute des évaluations de la règle à la fréquence que vous choisissez, par exemple toutes les 24 heures.
Hybride	Certaines règles comportent à la fois des changements de configuration et des déclencheurs périodiques. Pour ces règles, AWS Config évalue vos ressources lorsqu'il détecte un changement de configuration et également à la fréquence que vous spécifiez.

Modes d'évaluation

Il existe deux modes d'évaluation des AWS Config règles.

Mode d'évaluation	Description
Proactif	Utilisez l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriété s de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région.

Mode d'évaluation	Description
	Pour plus d'informations, consultez Modes d'évaluation. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.
Détective	Utilisez l'évaluation détective pour évaluer les ressources déjà déployées. Ce type d'évaluat ion vous permet d'évaluer les paramètres de configuration de vos ressources existantes.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Gestion des ressources supprimées à l'aide de AWS Config règles Lambda personnalisées

Les règles signalant les ressources supprimées doivent renvoyer le résultat de l'évaluation `NOT_APPLICABLE` afin d'éviter des évaluations de règles inutiles.

Lorsque vous supprimez une ressource, AWS Config crée un `configurationItem` avec `ResourceDeleted` pour`configurationItemStatus`. Vous pouvez utiliser ces métadonnées pour vérifier si une règle signale une ressource supprimée. Pour plus d'informations sur les éléments de configuration, consultez Concepts | Éléments de configuration.

Incluez les extraits de code suivants pour vérifier les ressources supprimées et définissez le résultat de l'évaluation d'une règle Lambda AWS Config personnalisée sur le fait qu'elle indique une ressource supprimée : `NOT_APPLICABLE`

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
```

```
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config les règles gérées et les règles de politique AWS Config personnalisées gèrent ce comportement par défaut.
> Si vous créez une règle lambd AWS Config personnalisée avec Python à l'aide du kit de AWS Config développement (RDK) et de la bibliothèque AWS Config du kit de développement (RDKlib), la classe Evaluator importée vérifiera ce comportement. Pour en savoir plus sur l'écriture des règles avec le RDK et le RDKLib, consultez Écriture de règles avec le RDK et le RDKLib.

Rubriques

- Création de règles de politique AWS Config personnalisées
- CréationAWS ConfigRègles Lambda personnalisées

Création de règles de politique AWS Config personnalisées

Vous pouvez créer des règles de politique AWS Config personnalisées à partir de l' AWS Config API AWS Management Console AWS CLI, ou. Pour plus d'informations sur la façon d'écrire des règles avec Guard, consultez la section Règles de Writing Guard dans le guide de l'utilisateur de AWS CloudFormation Guard. Pour plus d'informations sur les schémas des types de ressources pris en charge qui AWS Config peuvent être évalués, consultez la section types de ressources dans le référentiel des schémas de AWS Config ressources. GitHub

> **Important**
>
> Le schéma de AWS Config ressources pour évaluer les éléments de configuration est différent du schéma CFN pour évaluer les AWS CloudFormation modèles. Si vous utilisez le schéma CFN pour les règles de politiques AWS Config personnalisées, votre évaluation renverra le résultat `NOT_APPLICABLE`. Utilisez le schéma de AWS Config ressources lors de la création de règles de politique AWS Config personnalisées et rédigez des politiques en fonction de la structure des éléments de configuration. Pour obtenir la liste des schémas de AWS Config ressources, consultez la section types de ressources dans le référentiel de schémas de AWS Config ressources. GitHub

Création de règles de politique AWS Config personnalisées (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une AWS région qui prend en charge les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation de gauche, choisissez Règles.
4. Sur la page Règles, choisissez Ajouter une règle.
5. Sur la page Spécifier le type de règle, choisissez Créer une règle personnalisée à l'aide de Guard.
6. Sur la page Configurer une règle, créez la règle en réalisant les étapes suivantes :
   a. Saisissez un nom unique dans le champ Nom de la règle.

b. Saisissez une description de la règle dans le champ Description.

c. Pour la version d'exécution de Guard, choisissez le système d'exécution pour votre règle de politique AWS Config personnalisée.

d. Vous pouvez renseigner le Contenu de la règle avec la politique Guard personnalisée correspondant à votre règle. Pour plus d'informations sur la structure et les fonctionnalités des politiques personnalisées de AWS CloudFormation Guard, consultez les modes de fonctionnement de Guard 2.0 dans le GitHub référentiel Guard.

> **Note**
>
> Le schéma de AWS Config ressources pour évaluer les éléments de configuration est différent du schéma CFN pour évaluer les AWS CloudFormation modèles. Si vous utilisez le schéma CFN pour les règles de politiques AWS Config personnalisées, votre évaluation renverra le résultat `NOT_APPLICABLE`. Utilisez le schéma de AWS Config ressources lors de la création de règles de politique AWS Config personnalisées et rédigez des politiques en fonction de la structure des éléments de configuration. Pour une liste des schémas de AWS Config ressources, voir types de ressources dans le référentiel de schémas de AWS Config ressources. GitHub

L'exemple suivant montre la définition de politique pour une version de règle de politique AWS Config personnalisée de la règle AWS Config gérée dynamodb-pitr-enabled

```
# This rule checks if point in time recovery (PITR) is enabled on active Amazon
 DynamoDB tables
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
        let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription
        %pitr == "ENABLED"
```

```
}
```

e. Pour le mode d'évaluation, choisissez à quel moment du processus de création et de gestion des ressources vous AWS Config souhaitez évaluer vos ressources. Selon la règle, AWS Config vous pouvez évaluer vos configurations de ressources avant qu'une ressource ne soit provisionnée, après qu'une ressource ait été provisionnée, ou les deux.

   i. Choisissez Activer l'évaluation proactive pour évaluer les paramètres de configuration de vos ressources avant leur déploiement.

      Après avoir activé l'évaluation proactive, vous pouvez utiliser l'API StartResourced'évaluation et l'GetResourceEvaluationSummaryAPI pour vérifier si les ressources que vous spécifiez dans ces commandes seront signalées comme NON_COMPLIANT par les règles proactives de votre compte dans votre région.

      Pour plus d'informations sur l'utilisation de ces commandes, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.

   ii. Choisissez Activer l'évaluation détective pour évaluer les paramètres de configuration de vos ressources existantes.

      À des fins d'évaluation préventive, les règles de politique AWS Config personnalisée sont initiées par les modifications de configuration. Cette option sera présélectionnée.

      - Ressources : lorsqu'une ressource qui correspond au type de ressource spécifié, ou au type plus à l'identifiant, est créée, modifiée ou supprimée.
      - Balises : lorsqu'une ressource portant la balise spécifiée est créée, modifiée ou supprimée.
      - Toutes les modifications : lorsqu'une ressource enregistrée par AWS Config est créée, modifiée ou supprimée.

      AWS Config exécute l'évaluation lorsqu'il détecte une modification apportée à une ressource correspondant au champ d'application de la règle. Vous pouvez utiliser la portée afin de limiter les ressources qui déclenchent des évaluations. Dans le cas contraire, les évaluations sont lancées en cas de modification d'une ressource post-provisionnée.

   f. Vous pouvez personnaliser les valeurs des clés fournies dans le champ Paramètres, si votre règle comprend des paramètres. Un paramètre est un attribut que vos ressources doivent respecter pour pouvoir être considérées conformes à la règle.

7. Sur la page Réviser et créer, passez en revue toutes vos sélections avant d'ajouter la règle à votre Compte AWS.
8. Lorsque vous avez vérifié vos règles, choisissez Ajouter une règle.

Création de règles de politique AWS Config personnalisées (AWS CLI)

Utilisez la commande `put-config-rule`.

Le champ `Owner` doit présenter la valeur `CUSTOM_POLICY`. Les champs supplémentaires suivants sont obligatoires pour les règles de politique AWS Config personnalisée :

- `Runtime`: le système d'exécution de vos règles de politique AWS Config personnalisée.
- `PolicyText` : la définition de la politique contenant la logique de vos règles de politiques AWS Config personnalisées.
- `EnableDebugLogDelivery`: expression booléenne permettant d'activer la journalisation du débogage pour votre règle de politique AWS Config personnalisée. La valeur par défaut est `false`.

Création de règles de politique AWS Config personnalisées (API)

Utilisez l'action PutConfigRègle.

Le champ `Owner` doit présenter la valeur `CUSTOM_POLICY`. Les champs supplémentaires suivants sont obligatoires pour les règles de politique AWS Config personnalisée :

- `Runtime`: le système d'exécution de vos règles de politique AWS Config personnalisée.
- `PolicyText` : la politique qui définit la logique de vos règles de politiques AWS Config personnalisées.
- `EnableDebugLogDelivery`: expression booléenne permettant d'activer la journalisation du débogage pour votre règle de politique AWS Config personnalisée. La valeur par défaut est `false`.

CréationAWS ConfigRègles Lambda personnalisées

Vous pouvez développer des règles personnalisées et les ajouter àAWS ConfigavecAWS LambdaFonctions Vous associez chaque règle personnalisée à une fonction Lambda, qui contient la logique qui évalue si votreAWSles ressources sont conformes à la règle. Vous associez cette fonction à votre règle qui invoque la fonction soit en réponse aux changements de configuration, soit de façon périodique. La fonction évalue ensuite si vos ressources sont conformes à votre règle et elle envoie ses résultats d'évaluation à AWS Config.

L'exemple dansRègles Lambda personnalisées (exemple Amazon EC2)vous guide dans la création d'une règle Lambda personnalisée pour la première fois qui évalue si chacune de vos instances EC2 est du type t2.micro. Il inclut un exemple de fonction Lambda que vous pouvez ajouter àAWS Lambdasans aucune modification. L'exemple dansRègles Lambda personnalisées (exemple général)fournit un exemple plus général pour créer une règle Lambda personnalisée.

Pour savoir comment procéderAWS Lambdales fonctions fonctionnent et comment les développer, voirAWS LambdaManuel du développeur.

Rubriques

- Règles Lambda personnalisées (exemple Amazon EC2)
- Règles Lambda personnalisées (exemple général)
- Exemples de fonctions et d'événements AWS Lambda pour les règles AWS Config

Règles Lambda personnalisées (exemple Amazon EC2)

Cette procédure vous guide tout au long du processus de création d'une règle Lambda personnalisée qui évalue si chacune de vos instances EC2 est du type t2.micro. AWS Config exécutera des évaluations basées sur les événements pour cette règle, ce qui signifie qu'il vérifiera les configurations de votre instance chaque fois qu'un changement de configuration est AWS Config détecté dans une instance. AWS Config signalera les instances t2.micro comme conformes et toutes les autres instances comme non conformes. L'état de conformité apparait dans la console AWS Config .

Pour obtenir les meilleurs résultats avec cette procédure, vous devez disposer d'une ou de plusieurs instances EC2 dans votre Compte AWS. Vos instances doivent inclure une combinaison d'au moins une instance t2.micro et d'autres types.

Pour créer cette règle, vous devez d'abord créer une AWS Lambda fonction en personnalisant un plan dans la AWS Lambda console. Ensuite, vous allez créer une règle Lambda personnalisée dans AWS Config, et vous associerez la règle à la fonction.

Rubriques

- Création d'une fonction AWS Lambda pour une règle de configuration personnalisée
- Création d'une règle Lambda personnalisée pour évaluer les instances Amazon EC2

Création d'une fonction AWS Lambda pour une règle de configuration personnalisée

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région compatible avec les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans la AWS Lambda console, choisissez Create a Lambda function.
4. Choisissez Utiliser un plan. Dans la barre de recherche, saisissez config-rule-change-triggered. Sélectionnez le plan dans les résultats de filtre, puis choisissez Configurer.
5. Sur la page Configure triggers (Configurer les déclencheurs), choisissez Next (Suivant).
6. Sur la page Basic information, effectuez les étapes suivantes :
   a. Pour Nom de la fonction, entrez **`InstanceTypeCheck`**.
   b. Pour le rôle d'exécution, choisissez Créer un nouveau rôle à partir des modèles de AWS politique.
   c. Pour Runtime, conservez Node.js.
   d. Saisissez un nom dans le champ Nom de rôle.
   e. Pour Modèles de stratégie, choisissez Autorisations de règles AWS Config .
   f. Conservez le code préconfiguré pour la Fonction de code de fonction Lambda. Le code Node.js de votre fonction est fourni dans l'éditeur de code. Pour cette procédure, vous n'avez pas besoin de changer le code.
   g. Vérifiez les détails, puis choisissez Créer une fonction. La AWS Lambda console affiche votre fonction.

7. Pour vérifier que votre fonction est configurée correctement, testez-la avec les étapes ci-dessous :

   a. Choisissez Test dans le menu sous Présentation de la fonction, puis sélectionnez Configurer l'événement de test.

   b. Dans Modèle, choisissez Notification de changement d'élément de configuration AWS Config .

   c. Pour Name (Nom), tapez un nom.

   d. Choisissez Test. AWS Lambda teste votre fonction avec l'exemple d'événement. Si votre fonction est traitée comme prévu, un message d'erreur comme le suivant s'affiche sous Résultat de l'exécution :

   ```
   {
     "errorType": "InvalidResultTokenException,"
     "errorMessage": "Result Token provided is invalid",
   . . .
   ```

   Ceci `InvalidResultTokenException` est attendu car votre fonction ne s'exécute correctement que lorsqu'elle reçoit un jeton de résultat de AWS Config. Le jeton de résultats identifie la règle AWS Config et l'événement qui a provoqué l'évaluation. Ensuite, il associe une évaluation à une règle. Cette exception indique que votre fonction a les autorisations nécessaires pour envoyer les résultats à AWS Config. Sinon, le message d'erreur suivant s'affiche : `not authorized to perform: config:PutEvaluations`. Si cette erreur survient, mettez à jour le rôle que vous avez attribué à votre fonction pour autoriser l'action `config:PutEvaluations` et testez de nouveau votre fonction.

Création d'une règle Lambda personnalisée pour évaluer les instances Amazon EC2

1. Ouvrez la AWS Config console à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur la même région que celle dans laquelle vous avez créé la AWS Lambda fonction pour votre règle Lambda personnalisée.
3. Sur la page Règles, choisissez Ajouter une règle.
4. Sur la page Spécifier le type de règle, choisissez Créer une règle personnalisée.
5. Sur la page Configure rule (Configurer une règle), complétez les étapes suivantes :

a. Pour Nom, tapez **`InstanceTypesAreT2micro`**.

b. Pour Description, saisissez **`Evaluates whether EC2 instances are the t2.micro type`**.

c. Pour ARN de fonction AWS Lambda , spécifiez l'ARN qu' AWS Lambda a assigné à votre fonction.

> **Note**
>
> L'ARN que vous spécifiez à cette étape ne doit pas inclure le qualificateur `$LATEST`. Vous pouvez spécifier un ARN sans qualificatif de version ou avec un autre qualificatif`$LATEST`. AWS Lambda prend en charge le versionnement des fonctions, et chaque version se voit attribuer un ARN avec un qualificatif. AWS Lambda utilise le `$LATEST` qualificatif correspondant à la dernière version.

d. Pour Type de déclencheur, choisissez Lors de changements de configuration.

e. Pour Scope of changes (Portée des modifications), choisissez Ressources.

f. Pour Ressources, choisissez AWS Instance EC2 dans la liste déroulante Type de ressource.

g. Dans la section Paramètres, vous devez spécifier le paramètre de règle évalué par votre AWS Lambda fonction ainsi que la valeur souhaitée. La fonction de cette procédure évalue le paramètre `desiredInstanceType`.

   Pour Clé, tapez **`desiredInstanceType`**. Pour Valeur, tapez **`t2.micro`**.

6. Choisissez Suivant. Sur la page Vérifier et créer, vérifiez les détails de votre règle et choisissez Ajouter une fonction de règle. Votre nouvelle règle s'affiche sur la page Règles.

   La conformité s'affichera Évaluer... jusqu'à ce qu'il AWS Config reçoive les résultats d'évaluation de votre AWS Lambda fonction. Si la règle et la fonction fonctionnent comme prévu, un résumé des résultats s'affiche au bout de quelques minutes. Par exemple, le résultat 2 noncompliant resource(s) indique que 2 de vos instances ne sont pas des instances t2.micro et le résultat Conforme indique que toutes les instances sont de type t2.micro. Vous pouvez mettre à jour les résultats avec le bouton Refresh.

   Si la règle ou la fonction ne fonctionnent pas comme prévu, vous pouvez voir l'un des messages suivants pour Conformité :

- Aucun résultat n'a été signalé. Vos ressources ont AWS Config été évaluées par rapport à la règle. Cette règle ne s'appliquait à aucune des ressources AWS figurant dans sa portée, les ressources spécifiées ou les résultats de l'évaluation ont été supprimés. Pour obtenir les résultats de l'évaluation, mettez à jour la règle, modifiez sa portée ou choisissez Re-evaluate (Réévaluer).

  Vérifiez que la portée comprend Instance AWS EC2 pour Ressources et réessayez.
- Aucune ressource dans le champ d'application : AWS Config impossible d'évaluer vos AWS ressources enregistrées par rapport à cette règle car aucune de vos ressources n'entre dans le champ d'application de la règle. Pour obtenir les résultats de l'évaluation, modifiez la règle et sa portée, ou ajoutez des ressources AWS Config à enregistrer à l'aide de la page Paramètres.

  Vérifiez que les AWS Config instances EC2 sont enregistrées.
- Evaluations failed (Échec des évaluations) - pour obtenir des informations susceptibles de vous aider à déterminer le problème, choisissez le nom de la règle pour ouvrir sa page de détails et voir le message d'erreur.

Si votre règle fonctionne correctement et AWS Config fournit des résultats d'évaluation, vous pouvez découvrir quelles conditions affectent le statut de conformité de votre règle. Vous pouvez découvrir quelles ressources sont non conformes, le cas échéant, et pourquoi. Pour plus d'informations, voir Affichage des informations de conformité et des résultats d'évaluation.

Règles Lambda personnalisées (exemple général)

Effectuez la procédure suivante pour créer une règle Lambda personnalisée. Pour créer une règle Lambda personnalisée, vous devez d'abord créer une AWS Lambda fonction contenant la logique d'évaluation de la règle. Puis vous associez la fonction à une règle Lambda personnalisée que vous créez dans AWS Config.

> **Important**
>
> Pour des raisons de sécurité, lorsque vous AWS Config autorisez l'appel de votre fonction Lambda, nous vous recommandons vivement de restreindre l'accès dans la politique basée sur les ressources pour Lambda avec `sourceARN` et/ou dans la demande d'appel.

`sourceAccountId` Pour plus d'informations, consultez Bonnes pratiques de sécurité pour la politique AWS Lambda basée sur les ressources.

Table des matières

- Création d'une fonction AWS Lambda pour une règle de configuration personnalisée
- Création d'une règle personnalisée dans AWS Config
- Bonnes pratiques de sécurité pour la politique AWS Lambda basée sur les ressources
- Évaluation des types de ressources supplémentaires

Création d'une fonction AWS Lambda pour une règle de configuration personnalisée

Une fonction Lambda est un code personnalisé que vous téléchargez et qui est invoqué par des événements publiés par une source d'événements. AWS Lambda Si la fonction Lambda est associée à une règle Config, elle l' AWS Config invoque lorsque le déclencheur de la règle se produit. La fonction Lambda évalue ensuite les informations de configuration qui sont envoyées par AWS Config et elle retourne les résultats de l'évaluation. Pour plus d'informations sur les fonctions Lambda, consultez Fonction et sources d'événements dans le Guide du développeur AWS Lambda .

Vous pouvez utiliser un langage de programmation pris en charge par AWS Lambda pour créer une fonction Lambda pour une règle Lambda personnalisée. Pour faciliter cette tâche, vous pouvez personnaliser un AWS Lambda plan ou réutiliser un exemple de fonction du GitHub référentiel de AWS Config règles.

Plans AWS Lambda

La AWS Lambda console fournit des exemples de fonctions, ou plans, que vous pouvez personnaliser en ajoutant votre propre logique d'évaluation. Lorsque vous créez une fonction, vous pouvez choisir parmi les plans suivants :

- config-rule-change-triggered— Déclenché lorsque la configuration de vos AWS ressources change.
- config-rule-periodic— Déclenché à la fréquence que vous choisissez (par exemple, toutes les 24 heures).

AWS Config GitHub Référentiel de règles

Un référentiel public d'exemples de fonctions pour les règles Lambda personnalisées est disponible sur GitHub un service Web d'hébergement et de partage de code. Les exemples de fonctions sont

développés et fournis par la AWS communauté. Si vous souhaitez utiliser un exemple, vous pouvez copier son code dans une nouvelle AWS Lambda fonction. Pour afficher le référentiel, consultez https://github.com/awslabs/aws-config-rules/.

Pour créer la fonction pour votre règle personnalisée

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région compatible avec les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Choisissez Create a Lambda function.
4. Sur la page Utiliser un plan, vous pouvez choisir l'une des fonctions du plan pour les AWS Config règles comme point de départ, ou vous pouvez continuer sans plan en choisissant Ignorer.
5. Sur la page Configure triggers (Configurer les déclencheurs), choisissez Next (Suivant).
6. Sur la page Informations de base, saisissez un nom et une description.
7. Pour Runtime, choisissez le langage de programmation dans lequel votre fonction est écrit.
8. Pour Type d'entrée de code, choisissez votre type d'entrée préféré. Si vous utilisez un plan, conservez le code préconfiguré.
9. Fournissez votre code à l'aide de la méthode requise par le type d'entrée de code que vous avez sélectionné. Si vous utilisez un plan, le code de fonction est fourni dans l'éditeur de code et vous pouvez le personnaliser afin d'inclure votre propre logique d'évaluation. Votre code peut évaluer les données d'événement AWS Config fournies lorsqu'il appelle votre fonction :

   - Pour les fonctions basées sur le config-rule-change-triggeredplan ou pour les fonctions déclenchées par des modifications de configuration, les données d'événement sont l'élément de configuration ou un objet d'élément de configuration surdimensionné correspondant à la AWS ressource modifiée.
   - Pour les fonctions basées sur le config-rule-periodicplan ou pour les fonctions déclenchées à la fréquence que vous choisissez, les données d'événement sont un objet JSON qui inclut des informations sur le moment où l'évaluation a été déclenchée.
   - Pour les deux types de fonctions, AWS Config transmet les paramètres des règles au format JSON. Vous pouvez définir quels paramètres de la règle sont transmis lorsque vous créez la règle Lambda personnalisée dans AWS Config.

- Par exemple, les AWS Config événements publiés lorsqu'il appelle votre fonction, voirExemple d'événements pour les règles d' AWS Config.

10. Dans Rôle d'exécution, choisissez Créer un rôle à partir de modèles de politique AWS .
11. Tapez un nom pour Role name (Nom de rôle).
12. Pour Modèles de stratégie, choisissez Autorisations AWS Config Rules.
13. Vérifiez les détails, puis choisissez Créer une fonction.

Création d'une règle personnalisée dans AWS Config

AWS Config À utiliser pour créer une règle Lambda personnalisée et associer la règle à une fonction Lambda.

Pour créer une règle personnalisée

1. Ouvrez la AWS Config console à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur la même région que celle dans laquelle vous avez créé la AWS Lambda fonction pour votre règle Lambda personnalisée.
3. Sur la page Règles, choisissez Ajouter une règle.
4. Sur la page Spécifier le type de règle, choisissez Créer une règle personnalisée.
5. Sur la page Configure rule (Configurer une règle), saisissez un nom et une description.
6. Pour ARN de fonction AWS Lambda , spécifiez l'ARN qu' AWS Lambda a assigné à votre fonction.

> **Note**
>
> L'ARN que vous spécifiez à cette étape ne doit pas inclure le qualificateur `$LATEST`. Vous pouvez spécifier un ARN sans qualificatif de version ou avec un autre qualificatif`$LATEST`. AWS Lambda prend en charge le versionnement des fonctions, et chaque version se voit attribuer un ARN avec un qualificatif. AWS Lambda utilise le `$LATEST` qualificatif correspondant à la dernière version.

7. Pour Type de déclencheur, choisissez un ou les deux éléments suivants :
   - Modifications de configuration AWS Config : appelle votre fonction Lambda lorsqu'elle détecte un changement de configuration.

- AWS Config Périodique : invoque votre fonction Lambda à la fréquence que vous choisissez (par exemple, toutes les 24 heures).

8. Si les types de déclencheurs de votre règle incluent des modifications de configuration, spécifiez l'une des options suivantes pour Étendue des modifications avec laquelle AWS Config votre fonction Lambda est appelée :

   - Toutes les modifications : lorsqu'une ressource enregistrée par AWS Config est créée, modifiée ou supprimée.
   - Ressources : lorsqu'une ressource qui correspond au type spécifié, ou au type plus à l'identifiant, est créée, modifiée ou supprimée.
   - Balises : lorsqu'une ressource portant la balise spécifiée est créée, modifiée ou supprimée
9. Si les types de déclencheurs de votre règle incluent Periodic, spécifiez la fréquence à laquelle votre fonction Lambda est AWS Config invoquée.
10. Dans la section Paramètres, spécifiez tous les paramètres de règle évalués par votre AWS Lambda fonction ainsi que la valeur souhaitée.
11. Choisissez Suivant. Sur la page Vérifier et créer, vérifiez les détails de votre règle et choisissez Ajouter une fonction de règle. Votre nouvelle règle s'affiche sur la page Règles.

    La conformité s'affichera Évaluer... jusqu'à ce qu'il AWS Config reçoive les résultats d'évaluation de votre AWS Lambda fonction. Si la règle et la fonction fonctionnent comme prévu, un résumé des résultats s'affiche au bout de quelques minutes. Vous pouvez mettre à jour les résultats avec le bouton Refresh.

    Si la règle ou la fonction ne fonctionnent pas comme prévu, vous pouvez voir l'un des messages suivants pour Conformité :

    - Aucun résultat n'a été signalé. Vos ressources ont AWS Config été évaluées par rapport à la règle. Cette règle ne s'appliquait à aucune des ressources AWS figurant dans sa portée, les ressources spécifiées ou les résultats de l'évaluation ont été supprimés. Pour obtenir les résultats de l'évaluation, mettez à jour la règle, modifiez sa portée ou choisissez Re-evaluate (Réévaluer).

      Ce message peut également apparaître si la règle n'a pas renvoyé de résultats d'évaluation.
    - Aucune ressource dans le champ d'application : AWS Config impossible d'évaluer vos AWS ressources enregistrées par rapport à cette règle car aucune de vos ressources n'entre dans le champ d'application de la règle. Vous pouvez choisir quelles ressources AWS Config enregistre sur la page Paramètres.

- Evaluations failed (Échec des évaluations) - pour obtenir des informations susceptibles de vous aider à déterminer le problème, choisissez le nom de la règle pour ouvrir sa page de détails et voir le message d'erreur.

> **Note**
>
> Lorsque vous créez une règle Lambda personnalisée avec la AWS Config console, les autorisations appropriées sont automatiquement créées pour vous. Si vous créez une règle Lambda personnalisée avec le AWS CLI, vous devez AWS Config autoriser l'appel de votre fonction Lambda à l'aide de la commande. `aws lambda add-permission` Pour plus d'informations, consultez la section Utilisation de politiques basées sur les ressources pour (politiques de fonction AWS Lambda Lambda) dans le manuel du développeur.AWS Lambda Avant d' AWS Config autoriser l'appel de votre fonction Lambda, consultez la section suivante. Bonnes pratiques de sécurité pour la politique AWS Lambda basée sur les ressources

Bonnes pratiques de sécurité pour la politique AWS Lambda basée sur les ressources

En vertu des bonnes pratiques, pour éviter d'accorder à l'ensemble du nom du principal de service (SPN) l'autorisation d'invoquer votre fonction Lambda, nous vous recommandons vivement de restreindre l'accès dans la politique basée sur les ressources pour Lambda avec `sourceARN` et/ou `sourceAccountId` dans la demande d'appel.

`sourceARN`Il s'agit de l'ARN de la AWS Config règle qui invoque la fonction Lambda.

L'`sourceAccountId` est l'ID de compte de l'utilisateur qui a créé la règle.

La restriction de l'accès dans la politique basée sur les ressources Lambda permet de s'assurer que l'accès à vos ressources AWS Lambda est réservé aux utilisateurs et aux scénarios attendus.

Pour ajouter une autorisation basée sur le SPN, vous devez utiliser la CLI suivante

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com
```

Pour ajouter une autorisation SourceAccountId basée

Avant de créer la règle, vous pouvez ajouter une autorisation basée sur `sourceAccountId` à la politique basée sur les ressources à l'aide de la CLI suivante

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID
```

Pour ajouter à la fois une autorisation SourceArn et une autorisation SourceAccountId basée sur

Une fois la règle créée, vous pouvez ajouter une autorisation basée sur `sourceARN` à la politique basée sur les ressources à l'aide de la CLI suivante. Ainsi, seul un ARN de règle spécifique peut invoquer la fonction Lambda.

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID --source-arn ARN of the created config rule
```

Évaluation des types de ressources supplémentaires

Vous pouvez créer des règles Lambda personnalisées pour exécuter des évaluations pour des types de ressources qui n'ont pas encore été enregistrés par. AWS Config Cela est utile si vous souhaitez évaluer la conformité de types de ressources supplémentaires qui AWS Config ne sont pas enregistrés actuellement. Pour obtenir une liste des types de ressources supplémentaires que vous pouvez évaluer avec des règles Lambda personnalisées, consultez Référence des types de ressources AWS.

> **Note**
>
> Lorsque vous créez un Lambda personnalisé pour un type de ressource qui n'est pas enregistré par AWS Config, la règle doit avoir le type de déclencheur périodique. Le type de déclencheur des modifications de configuration n'est pas pris en charge. Pour plus d'informations, consultez Mode d'évaluation et types de déclencheurs pour les AWS Config règles.

Exemple

1. Vous souhaitez évaluer les coffres-forts Amazon S3 Glacier dans votre compte. Les ressources du coffre-fort Amazon S3 Glacier ne sont actuellement pas enregistrées par AWS Config.

2. Vous créez une AWS Lambda fonction qui évalue si vos coffres-forts Amazon S3 Glacier sont conformes aux exigences de votre compte.
3. Vous créez une règle Lambda personnalisée nommée, evaluate-glacier-vaultspuis vous lui attribuez votre AWS Lambda fonction.
4. AWS Config invoque votre fonction Lambda, puis évalue les coffres-forts Amazon S3 Glacier par rapport à votre règle.
5. AWS Config renvoie les évaluations et vous pouvez consulter les résultats de conformité de votre règle.

> **Note**
>
> Vous pouvez consulter les détails de configuration dans la AWS Config chronologie et rechercher les ressources compatibles dans la AWS Config AWS Config console. Si vous avez configuré AWS Config pour enregistrer tous les types de ressources, les nouvelles ressources prises en charge seront automatiquement enregistrées. Pour plus d'informations, voir Types de ressource pris en charge.

Exemples de fonctions et d'événements AWS Lambda pour les règles AWS Config

Chaque règle Lambda personnalisée est associée à une règle Lambdafonction, qui est un code personnalisé qui contient la logique d'évaluation de la règle. Lorsque le déclencheur d'une règle de Config se produit (par exemple, lorsqueAWS Configdétecte un changement de configuration),AWS Configinvoque la fonction Lambda de la règle en publiant unévénement, qui est un objet JSON qui fournit les données de configuration que la fonction évalue.

Pour de plus amples informations sur les fonctions et les événements dansAWS Lambda, consultezSources de fonctions et d'événementsdans leAWS LambdaManuel du développeur.

Rubriques

- Exemples de AWS Lambda fonctions pour AWS Config les règles (Node.js)
- Exemple de fonctions AWS Lambda pour les règles AWS Config (Python)
- Exemple d'événements pour les règles d' AWS Config

Exemples de AWS Lambda fonctions pour AWS Config les règles (Node.js)

AWS Lambda exécute des fonctions en réponse à des événements publiés par les AWS services. La fonction d'une règle Lambda AWS Config personnalisée reçoit un événement publié par AWS Config, puis utilise les données qu'elle reçoit de l'événement et qu'elle extrait de l' AWS Config API pour évaluer la conformité de la règle. Les opérations dans une fonction pour une règle de configuration varient selon qu'il s'agisse d'une évaluation déclenchée par des changements de configuration ou de façon périodique.

Pour plus d'informations sur les modèles courants au sein des AWS Lambda fonctions, voir Modèle de programmation dans le Guide du AWS Lambda développeur.

Table des matières

- Exemple de fonction pour des évaluations déclenchées par des changements de configuration
- Exemple de fonction pour des évaluations périodiques

Exemple de fonction pour des évaluations déclenchées par des changements de configuration

AWS Config invoquera une fonction comme dans l'exemple suivant lorsqu'elle détecte un changement de configuration pour une ressource comprise dans le champ d'application d'une règle personnalisée.

Si vous utilisez la AWS Config console pour créer une règle associée à une fonction comme dans cet exemple, choisissez Configuration changes comme type de déclencheur. Si vous utilisez l' AWS Config API ou AWS CLI pour créer la règle, définissez l'`MessageType`attribut sur `ConfigurationItemChangeNotification` et`OversizedConfigurationItemChangeNotification`. Ces paramètres permettent à votre règle d'être déclenchée chaque fois qu'un élément de configuration ou un élément de configuration surdimensionné est AWS Config généré à la suite d'un changement de ressource.

Cet exemple évalue vos ressources et vérifie si les instances correspondent au type de ressource, `AWS::EC2::Instance`. La règle est déclenchée quand AWS Config génère un élément de configuration ou une notification d'élément de configuration surdimensionné.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";
```

```
const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
```

```
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) =>
 {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
 false;
}

// In this example, the resource is compliant if it is an instance and its type matches
 the type specified as the desired type.
```

```
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is not
 compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
```

```
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

Opérations de la fonction

La fonction effectue les opérations suivantes lors de l'exécution :

1. La fonction s'exécute lorsque AWS Lambda l'`event`objet est transmis à la `handler` fonction. Dans cet exemple, la fonction accepte le `callback` paramètre facultatif, qu'elle utilise pour renvoyer des informations à l'appelant. AWS Lambda transmet également un `context` objet contenant des informations et des méthodes que la fonction peut utiliser pendant son exécution. Sachez que le contexte n'est plus utilisé dans les nouvelles versions de Lambda.
2. La fonction vérifie si le `messageType` pour l'événement est un élément de configuration ou un élément de configuration surdimensionné, puis renvoie l'élément de configuration.
3. Le gestionnaire appelle la fonction `isApplicable` afin de déterminer si la ressource a été supprimée.

> **Note**
>
> Les règles signalant les ressources supprimées doivent renvoyer le résultat de l'évaluation `NOT_APPLICABLE` afin d'éviter des évaluations de règles inutiles.

4. Le gestionnaire appelle la `evaluateChangeNotificationCompliance` fonction et transmet les `ruleParameters` objets `configurationItem` et AWS Config publiés lors de l'événement.

   La fonction commence par évaluer si la ressource est une instance EC2. Si la ressource n'est pas une instance EC2, la fonction renvoie la valeur de conformité `NOT_APPLICABLE`.

   La fonction évalue ensuite si l'attribut `instanceType` de l'élément de configuration est égal à la valeur du paramètre `desiredInstanceType`. Si les valeurs sont égales, la fonction renvoie `COMPLIANT`. Si les valeurs ne sont pas égales, la fonction renvoie `NON_COMPLIANT`.
5. Le gestionnaire se prépare à envoyer les résultats de l'évaluation à AWS Config en initialisant l'`putEvaluationsRequest`objet. Cet objet comprend le paramètre `Evaluations` qui identifie le résultat de la conformité, le type et l'ID de la ressource qui a été évaluée. L'`putEvaluationsRequest`objet inclut également le jeton de résultat de l'événement, qui identifie la règle et l'événement pour AWS Config.
6. Le gestionnaire envoie les résultats de l'évaluation à AWS Config en transmettant l'objet à la `putEvaluations` méthode du `config` client.

Exemple de fonction pour des évaluations périodiques

AWS Config invoquera une fonction comme dans l'exemple suivant pour les évaluations périodiques. Des évaluations périodiques se produisent à la fréquence que vous spécifiez lorsque vous définissez la règle dans AWS Config.

Si vous utilisez la AWS Config console pour créer une règle associée à une fonction comme dans cet exemple, choisissez Périodique comme type de déclencheur. Si vous utilisez l' AWS Config API ou AWS CLI pour créer la règle, définissez l'`MessageType`attribut sur`ScheduledNotification`.

Cet exemple vérifie si le nombre total d'une ressource donnée dépasse le maximum spécifié.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
 passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
```

```
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount, count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
```

```
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource type.",
 null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
```

```
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count, callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

Opérations de la fonction

La fonction effectue les opérations suivantes lors de l'exécution :

1. La fonction s'exécute lorsque AWS Lambda l'`event`objet est transmis à la `handler` fonction. Dans cet exemple, la fonction accepte le `callback` paramètre facultatif, qu'elle utilise pour renvoyer des informations à l'appelant. AWS Lambda transmet également un `context` objet contenant des informations et des méthodes que la fonction peut utiliser pendant son exécution. Sachez que le contexte n'est plus utilisé dans les nouvelles versions de Lambda.
2. Pour compter les ressources du type spécifié, le gestionnaire appelle la fonction `countResourceTypes` et il transmet le paramètre `applicableResourceType` qu'il a reçu de l'événement. La fonction `countResourceTypes` appelle la méthode `listDiscoveredResources` du client `config`, qui retourne une liste d'identificateurs pour les ressources applicables. La fonction utilise la longueur de cette liste pour déterminer le nombre de ressources applicables, et elle retourne ce nombre au gestionnaire.
3. Le gestionnaire se prépare à envoyer les résultats de l'évaluation à AWS Config en initialisant l'`putEvaluationsRequest`objet. Cet objet inclut le `Evaluations` paramètre, qui identifie le

résultat de conformité et celui Compte AWS qui a été publié lors de l'événement. Vous pouvez utiliser le paramètre `Evaluations` pour appliquer le résultat à n'importe quel type de ressource pris en charge par AWS Config. L'`putEvaluationsRequest`objet inclut également le jeton de résultat de l'événement, qui identifie la règle et l'événement pour AWS Config.

4. Au sein de l'objet `putEvaluationsRequest`, le gestionnaire appelle la fonction `evaluateCompliance`. Cette fonction teste si le nombre de ressources applicables dépasse le maximum attribué au paramètre `maxCount` fourni par l'événement. Si le nombre maximum de ressources est dépassé, la fonction renvoie `NON_COMPLIANT`. Si le nombre maximum de ressources n'est pas dépassé, la fonction renvoie `COMPLIANT`.
5. Le gestionnaire envoie les résultats de l'évaluation à AWS Config en transmettant l'objet à la `putEvaluations` méthode du `config` client.

Exemple de fonctions AWS Lambda pour les règles AWS Config (Python)

AWS Lambda exécute des fonctions en réponse à des événements qui sont publiés par des services d'AWS. La fonction d'une règle Lambda AWS Config personnalisée reçoit un événement qui est publié par AWS Config. La fonction utilise ensuite les données qu'elle reçoit de l'événement et qu'elle récupère dans l'API AWS Config pour évaluer la conformité de la règle. Les opérations dans une fonction pour une règle de configuration varient selon qu'il s'agisse d'une évaluation déclenchée par des changements de configuration ou de façon périodique.

Pour en savoir plus sur les modèles courants au sein des fonctions AWS Lambda, consultez Modèles de programmation dans le Guide du développeur AWS Lambda.

Table des matières

- Exemple de fonction pour des évaluations déclenchées par des changements de configuration
- Exemple de fonction pour des évaluations périodiques

Exemple de fonction pour des évaluations déclenchées par des changements de configuration

AWS Config appelle une fonction comme dans l'exemple suivant lorsqu'il détecte un changement de configuration au niveau d'une ressource qui se trouve dans l'étendue d'une règle personnalisée.

Si vous utilisez la console AWS Config pour créer une règle qui est associée à une fonction, comme dans cet exemple, choisissez Configuration changes (Changements de configuration) en tant que type de déclencheur. Si vous utilisez l'API AWS Config ou l'AWS CLI pour créer la règle, définissez l'attribut `MessageType` sur `ConfigurationItemChangeNotification` et

`OversizedConfigurationItemChangeNotification`. Ces paramètres permettent à votre règle d'être déclenchée dès qu'AWS Config génère un élément de configuration ou un élément de configuration surdimensionné à la suite d'un changement de ressource.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
```

```
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] = json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'], 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
```

```
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT
```

```
    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

Opérations de la fonction

La fonction effectue les opérations suivantes lors de l'exécution :

1. La fonction s'exécute lorsqu'AWS Lambda transmet l'objet `event` à la fonction `handler`. Dans cet exemple, la fonction accepte le paramètre facultatif `callback`, qu'elle utilise pour renvoyer des informations à l'appelant. AWS Lambda transmet également un objet `context` contenant des informations et des méthodes susceptibles d'être utilisés par la fonction pendant son exécution. Sachez que le contexte n'est plus utilisé dans les nouvelles versions de Lambda.
2. La fonction vérifie si le `messageType` pour l'événement est un élément de configuration ou un élément de configuration surdimensionné, puis renvoie l'élément de configuration.
3. Le gestionnaire appelle la fonction `isApplicable` afin de déterminer si la ressource a été supprimée.

> **Note**
>
> Les règles signalant les ressources supprimées doivent renvoyer le résultat de l'évaluation `NOT_APPLICABLE` afin d'éviter des évaluations de règles inutiles.

4. Le gestionnaire appelle la fonction `evaluateChangeNotificationCompliance` et passe les objets `configurationItem` et `ruleParameters` publiés par AWS Config dans l'événement.

   La fonction commence par évaluer si la ressource est une instance EC2. Si la ressource n'est pas une instance EC2, la fonction renvoie la valeur de conformité `NOT_APPLICABLE`.

   La fonction évalue ensuite si l'attribut `instanceType` de l'élément de configuration est égal à la valeur du paramètre `desiredInstanceType`. Si les valeurs sont égales, la fonction renvoie `COMPLIANT`. Si les valeurs ne sont pas égales, la fonction renvoie `NON_COMPLIANT`.
5. Le gestionnaire prépare l'envoi des résultats de l'évaluation à AWS Config en initialisant l'objet `putEvaluationsRequest`. Cet objet comprend le paramètre `Evaluations` qui identifie le résultat de la conformité, le type et l'ID de la ressource qui a été évaluée. L'objet `putEvaluationsRequest` comprend également le jeton du résultat de l'événement, qui permet l'identification de la règle et de l'événement par AWS Config.
6. Le gestionnaire envoie les résultats de l'évaluation à AWS Config en passant l'objet dans la méthode `putEvaluations` du client `config`.

Exemple de fonction pour des évaluations périodiques

AWS Config appelle une fonction comme dans l'exemple suivant pour des évaluations périodiques. Des évaluations périodiques se produisent à la fréquence que vous spécifiez lorsque vous définissez la règle dans AWS Config.

Si vous utilisez la console AWS Config pour créer une règle qui est associée à une fonction comme dans cet exemple, choisissez Periodic (Périodique) en tant que type de déclencheur. Si vous utilisez l'API AWS Config ou l'AWS CLI pour créer la règle, définissez l'attribut `MessageType` sur `ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime
```

```
# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
```

```
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value to
 the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report on
 the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):
```

```
    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
 resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
 ResultToken=event['resultToken'])
```

Opérations de la fonction

La fonction effectue les opérations suivantes lors de l'exécution :

1. La fonction s'exécute lorsqu'AWS Lambda transmet l'objet `event` à la fonction `handler`. Dans cet exemple, la fonction accepte le paramètre facultatif `callback`, qu'elle utilise pour renvoyer des informations à l'appelant. AWS Lambda transmet également un objet `context` contenant des informations et des méthodes susceptibles d'être utilisés par la fonction pendant son exécution. Sachez que le contexte n'est plus utilisé dans les nouvelles versions de Lambda.
2. Pour compter les ressources du type spécifié, le gestionnaire appelle la fonction `countResourceTypes` et il transmet le paramètre `applicableResourceType` qu'il a reçu de l'événement. La fonction `countResourceTypes` appelle la méthode

`listDiscoveredResources` du client `config`, qui retourne une liste d'identificateurs pour les ressources applicables. La fonction utilise la longueur de cette liste pour déterminer le nombre de ressources applicables, et elle retourne ce nombre au gestionnaire.

3. Le gestionnaire prépare l'envoi des résultats de l'évaluation à AWS Config en initialisant l'objet `putEvaluationsRequest`. Cet objet comprend le paramètre `Evaluations` qui identifie le résultat de conformité et le Compte AWS qui a été publié dans l'événement. Vous pouvez utiliser le paramètre `Evaluations` pour appliquer le résultat à n'importe quel type de ressource pris en charge par AWS Config. L'objet `putEvaluationsRequest` comprend également le jeton du résultat de l'événement, qui permet l'identification de la règle et de l'événement par AWS Config.
4. Au sein de l'objet `putEvaluationsRequest`, le gestionnaire appelle la fonction `evaluateCompliance`. Cette fonction teste si le nombre de ressources applicables dépasse le maximum attribué au paramètre `maxCount` fourni par l'événement. Si le nombre maximum de ressources est dépassé, la fonction renvoie `NON_COMPLIANT`. Si le nombre maximum de ressources n'est pas dépassé, la fonction renvoie `COMPLIANT`.
5. Le gestionnaire envoie les résultats de l'évaluation à AWS Config en passant l'objet dans la méthode `putEvaluations` du client `config`.

Exemple d'événements pour les règles d' AWS Config

Lorsque le déclencheur d'une règle se produit, AWS Config invoque la AWS Lambda fonction de la règle en publiant un événement. AWS Lambda Exécute ensuite la fonction en transmettant l'événement au gestionnaire de la fonction.

Exemple d'événement pour les évaluations déclenchées par des changements de configuration

AWS Config publie un événement lorsqu'il détecte un changement de configuration pour une ressource comprise dans le champ d'application d'une règle. L'exemple d'événement suivant montre que la règle a été déclenchée par une modification de la configuration d'une instance EC2.

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
```

```
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Exemple d'événement pour les évaluations déclenchées par des changements de configuration surdimensionnés

Certaines modifications de ressources génèrent des éléments de configuration surdimensionnés. L'exemple d'événement suivant montre que la règle a été déclenchée par une modification de la configuration surdimensionnée d'une instance EC2.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Exemple d'événement pour les évaluations déclenchées par une fréquence périodique

AWS Config publie un événement lorsqu'il évalue vos ressources à une fréquence que vous spécifiez (par exemple toutes les 24 heures). L'exemple d'événement suivant montre que la règle a été déclenchée par une fréquence périodique.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime\":
\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",\"recordVersion
\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Attributs d'événement

L'objet JSON d'un AWS Config événement contient les attributs suivants :

`invokingEvent`

L'événement qui déclenche l'évaluation d'une règle. Si l'événement est publié en réponse à un changement de configuration de ressource, la valeur de cet attribut est une chaîne qui contient un élément de configuration JSON `configurationItem` ou un `configurationItemSummary` (pour les éléments de configuration surdimensionnés). L'élément de configuration représente l'état de la ressource au moment où le changement a AWS Config été détecté. Pour un exemple d'élément de configuration, consultez le résultat produit par la `get-resource-config-history` AWS CLI commande dansAffichage de l'historique de configuration.

Si l'événement est publié pour une évaluation périodique, la valeur est une chaîne qui contient un objet JSON. L'objet comporte des informations sur l'évaluation qui a été déclenchée.

Pour chaque type d'événement, une fonction doit analyser la chaîne avec un analyseur JSON afin d'être en mesure d'évaluer son contenu, comme illustré dans l'exemple suivant de Node.js :

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Paires clé/valeur que la fonction traite dans le cadre de sa logique d'évaluation. Vous définissez des paramètres lorsque vous utilisez la AWS Config console pour créer une règle Lambda personnalisée. Vous pouvez également définir des paramètres avec l'`InputParameters`attribut dans la demande `PutConfigRule` AWS Config d'API ou dans la `put-config-rule` AWS CLI commande.

Le code JSON pour les paramètres est contenu dans une chaîne, donc une fonction doit analyser la chaîne avec un analyseur JSON afin d'être en mesure d'évaluer son contenu, comme illustré dans l'exemple suivant de Node.js :

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

Un jeton auquel la fonction doit être transmise AWS Config lors de l'`PutEvaluations`appel.

`eventLeftScope`

Valeur booléenne qui indique si la AWS ressource à évaluer a été supprimée du champ d'application de la règle. Si la valeur est `true`, la fonction indique que l'évaluation peut être ignorée en transmettant `NOT_APPLICABLE` en tant que valeur pour l'attribut `ComplianceType` dans l'appel de `PutEvaluations`.

`executionRoleArn`

L'ARN du rôle IAM attribué à AWS Config.

`configRuleArn`

L'ARN AWS Config attribué à la règle.

`configRuleName`

Le nom que vous avez attribué à la règle qui a entraîné la publication AWS Config de l'événement et l'appel de la fonction.

`configRuleId`

L'ID AWS Config attribué à la règle.

`accountId`

L'ID du propriétaire Compte AWS de la règle.

`version`

Numéro de version attribué par AWS. La version augmentera si des attributs sont AWS ajoutés aux AWS Config événements. Si une fonction requiert un attribut qui figure uniquement dans des événements qui correspondent à ou dépassent une version spécifique, cette fonction peut vérifier la valeur de cet attribut.

La version actuelle pour les AWS Config événements est 1.0.

Ajouter, mettre à jour et supprimer des AWS Config règles

Vous pouvez utiliser la AWS Config console ou les AWS kits SDK pour afficher, ajouter et supprimer vos règles.

Ajout, affichage, mise à jour et suppression de règles (console)

La page Règles affiche vos règles et leurs résultats de conformité actuels sous forme de tableau. Le résultat pour chaque règle est Evaluer... jusqu'à la AWS Config fin de l'évaluation de vos ressources par rapport à la règle. Vous pouvez mettre à jour les résultats avec le bouton Refresh. Lorsque AWS Config les évaluations sont terminées, vous pouvez voir les règles et les types de ressources conformes ou non conformes. Pour plus d'informations, consultez Affichage des informations de conformité et des résultats d'évaluation.

> **Note**
>
> AWS Config évalue uniquement les types de ressources qu'il enregistre. Par exemple, si vous ajoutez la règle compatible avec Cloudtrail mais que vous n'enregistrez pas le type de ressource de CloudTrail suivi, vous ne AWS Config pouvez pas évaluer si les sentiers de votre compte sont conformes ou non conformes. Pour plus d'informations, consultez AWS Ressources d'enregistrement.

Ajout de règles

Pour ajouter une règle

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région compatible avec les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation de gauche, choisissez Règles.
4. Sur la page Règles, choisissez Ajouter une règle.
5. Sur la page Spécifier le type de règle, indiquez le type de règle en effectuant les étapes suivantes :

   a. Commencez une saisie dans le champ de recherche pour filtrer la liste des règles gérées par nom de règle, description et étiquette. Par exemple, tapez EC2 pour renvoyer des règles permettant d'évaluer des types de ressources EC2 ou tapez périodique pour renvoyer des règles déclenchées de façon périodique.

   b. Vous pouvez également créer votre propre règles personnalisée. Choisissez Créer une règle personnalisée à l'aide de Lambda ou Créer une règle personnalisée à l'aide de Guard, puis suivez la procédure décrite dans Création de règles AWS Config Lambda personnalisées ou Création AWS Config de règles de politique personnalisées.
6. Sur la page Configurer une règle, configurez la règle en réalisant les étapes suivantes :

   a. Dans Nom, tapez un nom unique pour la règle.

   b. Saisissez une description de la règle dans le champ Description.

   c. Pour le mode d'évaluation, choisissez à quel moment du processus de création et de gestion des ressources vous AWS Config souhaitez évaluer vos ressources. Selon la règle, AWS Config vous pouvez évaluer vos configurations de ressources avant le déploiement d'une ressource, après le déploiement d'une ressource, ou les deux.

      i. Choisissez Activer l'évaluation proactive pour évaluer les paramètres de configuration de vos ressources avant leur déploiement.

         Après avoir activé l'évaluation proactive, vous pouvez utiliser l'API StartResourced'évaluation et l'GetResourceEvaluationSummaryAPI pour vérifier si les

ressources que vous spécifiez dans ces commandes seront signalées comme NON CONFORMES par les règles proactives de votre compte dans votre région.

Pour plus d'informations sur l'utilisation de ces commandes, consultez la section Évaluation de vos ressources à l'aide de AWS Config règles. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.

ii. Choisissez Activer l'évaluation détective pour évaluer les paramètres de configuration de vos ressources existantes.

Deux types de déclencheurs sont disponibles pour l'évaluation détective : Lors de changements de configuration et Périodique.

A. Si les types de déclencheurs de votre règle incluent des modifications de configuration, spécifiez l'une des options suivantes pour Étendue des modifications avec laquelle AWS Config votre fonction Lambda est appelée :

- Ressources : lorsqu'une ressource qui correspond au type de ressource spécifié, ou au type plus à l'identifiant, est créée, modifiée ou supprimée.
- Balises : lorsqu'une ressource portant la balise spécifiée est créée, modifiée ou supprimée.
- Toutes les modifications : lorsqu'une ressource enregistrée par AWS Config est créée, modifiée ou supprimée.

AWS Config exécute l'évaluation lorsqu'il détecte une modification apportée à une ressource correspondant au champ d'application de la règle. Vous pouvez utiliser la portée afin de définir les ressources qui déclenchent des évaluations.

B. Si les types de déclencheurs de votre règle incluent Periodic, spécifiez la fréquence à laquelle votre fonction Lambda est AWS Config invoquée.

d. Vous pouvez personnaliser les valeurs des clés fournies dans le champ Paramètres, si votre règle comprend des paramètres. Un paramètre est un attribut que vos ressources doivent respecter pour pouvoir être considérées conformes à la règle.

7. Sur la page Réviser et créer, passez en revue toutes vos sélections avant d'ajouter la règle à votre Compte AWS. Si la règle ne fonctionne pas comme prévu, l'un des messages suivants relatifs à la Conformité s'affiche :

- Aucun résultat n'a été signalé. Vos ressources ont AWS Config été évaluées par rapport à la règle. La règle ne s'appliquait pas aux AWS ressources incluses dans son champ d'application, les ressources spécifiées ont été supprimées ou les résultats de l'évaluation ont été supprimés. Pour obtenir les résultats de l'évaluation, mettez à jour la règle, modifiez sa portée ou choisissez Re-evaluate (Réévaluer).

  Ce message peut également apparaître si la règle n'a pas renvoyé de résultats d'évaluation.
- Aucune ressource dans le champ d'application : AWS Config impossible d'évaluer vos AWS ressources enregistrées par rapport à cette règle car aucune de vos ressources n'entre dans le champ d'application de la règle. Pour obtenir les résultats de l'évaluation, modifiez la règle et sa portée, ou ajoutez des ressources AWS Config à enregistrer à l'aide de la page Paramètres.
- Evaluations failed (Échec des évaluations) - pour obtenir des informations susceptibles de vous aider à déterminer le problème, choisissez le nom de la règle pour ouvrir sa page de détails et voir le message d'erreur.

Affichage des règles

Pour afficher vos règles

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région compatible avec les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation de gauche, choisissez Règles.
4. La page Règles affiche toutes les règles actuellement présentes dans votre Compte AWS. Le nom, les mesures correctives associées et l'état de conformité de chaque règle sont répertoriés.

   - Cliquez sur Ajouter une règle pour commencer à créer une règle.
   - Choisissez une règle pour consulter ses paramètres, ou choisissez une règle et sélectionnez Afficher les détails.
   - Consultez l'état de conformité de la règle lorsqu'elle évalue vos ressources.

- Choisissez une règle et l'option Modifier la règle pour modifier les paramètres de configuration de la règle et définir une mesure corrective pour une règle non conforme.

Mise à jour des règles

Pour mettre à jour une règle

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région compatible avec les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation de gauche, choisissez Règles.
4. Choisissez une règle et l'option Modifier la règle correspondant à la règle que vous souhaitez mettre à jour.
5. Modifiez les paramètres sur la page Modifier la règle pour modifier votre règle en fonction de vos besoins.
6. Choisissez Enregistrer.

Suppression de règles

Pour supprimer une règle

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région compatible avec les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation de gauche, choisissez Règles.
4. Choisissez la règle que vous souhaitez supprimer dans le tableau.
5. Dans la liste déroulante Actions, choisissez Supprimer une règle.
6. Lorsque vous y êtes invité, tapez « Supprimer » (cette entrée est sensible à la casse), puis choisissez Supprimer.

Activation de l'évaluation proactive

Vous pouvez utiliser l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriétés de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région.

Le schéma du type de ressource indique les propriétés d'une ressource. Vous pouvez trouver le schéma du type de ressource dans « extensions AWS publiques » du AWS CloudFormation registre ou à l'aide de la commande CLI suivante :

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Pour plus d'informations, consultez la section Gestion des extensions via le AWS CloudFormation registre et la référence aux types de AWS ressources et de propriétés dans le guide de AWS CloudFormation l'utilisateur.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Pour activer l'évaluation proactive

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région qui prend en charge les AWS Config règles. Pour obtenir la liste des régions AWS prises en charge, consultez Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation de gauche, choisissez Règles. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.
4. Choisissez une règle et l'option Modifier la règle correspondant à la règle que vous souhaitez mettre à jour.
5. Choisissez Activer l'évaluation proactive pour le Mode d'évaluation afin de pouvoir évaluer les paramètres de configuration de vos ressources avant leur déploiement.

6. Choisissez Enregistrer.

Après avoir activé l'évaluation proactive, vous pouvez utiliser l'API StartResourced'évaluation et l'GetResourceEvaluationSummaryAPI pour vérifier si les ressources que vous spécifiez dans ces commandes seront signalées comme NON CONFORMES par les règles proactives de votre compte dans votre région.

Par exemple, commencez par l' StartResourceEvaluation API :

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Vous devriez recevoir le `ResourceEvaluationId` dans la sortie :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Ensuite, utilisez l'API `ResourceEvaluationId` avec l' GetResourceEvaluationSummary API pour vérifier le résultat de l'évaluation :

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Votre résultat doit être similaire à ce qui suit :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
```

```
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Pour obtenir des informations supplémentaires sur le résultat de l'évaluation, telles que la règle qui a marqué une ressource comme NON_COMPLIANT, utilisez l'GetComplianceDetailsByAPI Resource.

Afficher, mettre à jour ou ajouter et supprimer des règles (AWS SDK)

Affichage des règles

Les exemples de code suivants montrent comment utiliser`DescribeConfigRules`.

CLI

AWS CLI

Pour obtenir les détails d'une règle AWS Config

La commande suivante renvoie les détails d'une règle AWS Config nommée `InstanceTypesAreT2micro` :

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

Sortie :

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
```

```
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Pour plus de détails sur l'API, consultez la section DescribeConfigRègles du manuel de référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple répertorie les règles de configuration du compte, avec les propriétés sélectionnées.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Sortie :

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                      ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                               config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
```

```
access-keys-rotated                                 config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required        config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Pour plus de détails sur l'API, consultez la section DescribeConfigRègles du manuel de référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
```

```
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Pour plus de détails sur l'API, consultez la section DescribeConfigRules in AWS SDK for Python (Boto3) API Reference.

Mise à jour ou ajout de règles

Les exemples de code suivants montrent comment utiliser`PutConfigRule`.

CLI

AWS CLI

Pour ajouter une règle Config AWS gérée

La commande suivante fournit du code JSON pour ajouter une règle de configuration AWS gérée :

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.jsonest` un fichier JSON qui contient la configuration des règles :

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
```

```
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Pour l'`ComplianceResourceTypes`attribut, ce code JSON limite la portée aux ressources de ce `AWS::EC2::Instance` type. AWS Config évaluera donc uniquement les instances EC2 par rapport à la règle. Comme la règle est une règle gérée, l'`Owner`attribut est défini sur`AWS`, et l'`SourceIdentifier`attribut est défini sur l'identifiant de règle,`REQUIRED_TAGS`. Pour l'`InputParameters`attribut, les clés de balise requises par la règle, `CostCenter` et`Owner`, sont spécifiées.

Si la commande aboutit, AWS Config ne renvoie aucune sortie. Pour vérifier la configuration des règles, exécutez la describe-config-rules commande et spécifiez le nom de la règle.

Pour ajouter une règle Config gérée par le client

La commande suivante fournit du code JSON pour ajouter une règle de configuration gérée par le client :

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`est un fichier JSON qui contient la configuration des règles :

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
```

```
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Pour l'`ComplianceResourceTypes`attribut, ce code JSON limite la portée aux ressources de ce `AWS::EC2::Instance` type. AWS Config évaluera donc uniquement les instances EC2 par rapport à la règle. Cette règle étant une règle gérée par le client, l'`Owner`attribut est défini sur`CUSTOM_LAMBDA`, et l'`SourceIdentifier`attribut est défini sur l'ARN de la fonction AWS Lambda. L'`SourceDetails`objet est obligatoire. Les paramètres spécifiés pour l'`InputParameters`attribut sont transmis à la fonction AWS Lambda lorsque AWS Config l'invoque pour évaluer les ressources par rapport à la règle.

Si la commande aboutit, AWS Config ne renvoie aucune sortie. Pour vérifier la configuration des règles, exécutez la describe-config-rules commande et spécifiez le nom de la règle.

- Pour plus de détails sur l'API, consultez la section PutConfigRègle dans le AWS CLI manuel de référence des commandes.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Pour plus de détails sur l'API, voir PutConfigRule in AWS SDK for Python (Boto3) API Reference.

Suppression de règles

Les exemples de code suivants montrent comment utiliser`DeleteConfigRule`.

CLI

AWS CLI

Pour supprimer une règle AWS Config

La commande suivante supprime une règle AWS Config nommée `MyConfigRule` :

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Pour plus de détails sur l'API, consultez la section DeleteConfigRègle dans le AWS CLI manuel de référence des commandes.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
```

```
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Pour plus de détails sur l'API, voir DeleteConfigRule in AWS SDK for Python (Boto3) API Reference.

Activer l'évaluation proactive (AWS CLI)

Vous pouvez utiliser l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriétés de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région.

Le schéma du type de ressource indique les propriétés d'une ressource. Vous pouvez trouver le schéma du type de ressource dans « extensions AWS publiques » du AWS CloudFormation registre ou à l'aide de la commande CLI suivante :

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Pour plus d'informations, consultez la section Gestion des extensions via le AWS CloudFormation registre et la référence aux types de AWS ressources et de propriétés dans le guide de AWS CloudFormation l'utilisateur.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Pour activer l'évaluation proactive

Utilisez la commande `put-config-rule` et activez `PROACTIVE` pour `EvaluationModes`.

Après avoir activé l'évaluation proactive, vous pouvez utiliser les commandes CLI start-resource-evaluation et get-resource-evaluation-summary CLI pour vérifier si les ressources que vous spécifiez dans ces commandes seront signalées comme NON_COMPLIANT par les règles proactives de votre compte dans votre région.

Commencez par exemple avec la commande start-resource-evaluation :

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Vous devriez recevoir le `ResourceEvaluationId` dans la sortie :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Utilisez ensuite l'`ResourceEvaluationId` avec get-resource-evaluation-summary pour vérifier le résultat de l'évaluation :

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Votre résultat doit être similaire à ce qui suit :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
```

```
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Pour obtenir des informations supplémentaires sur le résultat de l'évaluation, telles que la règle qui a marqué une ressource comme NON_COMPLIANT, utilisez la commande d'API get-compliance-details-by-resource.

> **Note**
>
> Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.

Activer l'évaluation proactive (API)

Vous pouvez utiliser l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriétés de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région.

Le schéma du type de ressource indique les propriétés d'une ressource. Vous pouvez trouver le schéma du type de ressource dans « extensions AWS publiques » du AWS CloudFormation registre ou à l'aide de la commande CLI suivante :

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Pour plus d'informations, consultez la section Gestion des extensions via le AWS CloudFormation registre et la référence aux types de AWS ressources et de propriétés dans le guide de AWS CloudFormation l'utilisateur.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Pour activer l'évaluation proactive d'une règle

Utilisez l'action PutConfigRègle et activez `PROACTIVE` pour`EvaluationModes`.

Après avoir activé l'évaluation proactive, vous pouvez utiliser l'API StartResourced'évaluation et l'GetResourceEvaluationSummaryAPI pour vérifier si les ressources que vous spécifiez dans ces commandes seront signalées comme NON CONFORMES par les règles proactives de votre compte dans votre région. Par exemple, commencez par l' StartResourceEvaluation API :

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Vous devriez recevoir le `ResourceEvaluationId` dans la sortie :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Ensuite, utilisez l'API `ResourceEvaluationId` avec l' GetResourceEvaluationSummary API pour vérifier le résultat de l'évaluation :

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Votre résultat doit être similaire à ce qui suit :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
```

```
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Pour obtenir des informations supplémentaires sur le résultat de l'évaluation, telles que la règle qui a marqué une ressource comme NON_COMPLIANT, utilisez l'GetComplianceDetailsByAPI Resource.

> **Note**
>
> Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.

Envoi d'évaluations de règles à Security Hub

Après avoir ajouté une AWS Config règle, vous pouvez également envoyer des évaluations de règles à AWS Security Hub. L'intégration entre Security Hub vous permet de trier AWS Config et de corriger les évaluations des règles ainsi que d'autres erreurs de configuration et problèmes de sécurité.

Envoi d'évaluations de règles à Security Hub

Pour envoyer des évaluations de règles à Security Hub, vous devez d'abord configurer AWS Security Hub puis AWS Config ajouter au moins une règle AWS Config gérée ou personnalisée. Ensuite, commence AWS Config immédiatement à envoyer les évaluations des règles à Security Hub. Security Hub enrichit les évaluations de règles et les transforme en résultats Security Hub.

Pour plus d'informations sur cette intégration, consultez la section Intégrations AWS de services disponibles dans le guide de l' AWS Security Hub utilisateur.

Évaluer vos ressources à l'aide de AWS Config règles

Lorsque vous créez des règles personnalisées ou que vous utilisez des règles gérées, vos ressources AWS Config sont évaluées par rapport à ces règles. Vous pouvez exécuter des évaluations à la demande pour les ressources par rapport à vos règles. Par exemple, cela est utile lorsque vous créez une règle personnalisée et que vous souhaitez vérifier AWS Config qu'elle évalue correctement vos ressources ou pour identifier s'il existe un problème avec la logique d'évaluation de votre AWS Lambda fonction.

Exemple

1. Vous créez une règle personnalisée qui évalue si vos utilisateurs IAM disposent de clés d'accès actives.
2. AWS Config évalue vos ressources par rapport à votre règle personnalisée.
3. Votre compte comporte un utilisateur IAM sans clé d'accès active. Votre règle ne signale pas correctement cette ressource comme NON_COMPLIANT.
4. Vous corrigez la règle et recommencez l'évaluation.
5. Étant donné que vous avez corrigé votre règle, celle-ci évalue correctement vos ressources et indique que la ressource d'utilisateur IAM est NON_COMPLIANT.

Lorsque vous ajoutez une règle à votre compte, vous pouvez indiquer à quel moment du processus de création et de gestion des ressources vous AWS Config souhaitez évaluer vos ressources. Le processus de création et de gestion des ressources est connu sous le nom de mise en service des ressources. Vous choisissez le mode d'évaluation pour spécifier à quel moment vous souhaitez évaluer vos ressources AWS Config au cours de ce processus.

Selon la règle, AWS Config vous pouvez évaluer vos configurations de ressources avant le déploiement d'une ressource, après le déploiement d'une ressource, ou les deux. L'évaluation d'une ressource avant son déploiement est une évaluation proactive. L'évaluation d'une ressource après son déploiement est une évaluation détective.

Mode proactif

Utilisez l'évaluation proactive pour évaluer les ressources avant leur déploiement. Cela vous permet d'évaluer si un ensemble de propriétés de ressources, s'il est utilisé pour définir une AWS ressource, serait CONFORME ou NON_COMPLIANT compte tenu de l'ensemble de règles proactives que vous avez dans votre compte dans votre région.

Le schéma du type de ressource indique les propriétés d'une ressource. Vous pouvez trouver le schéma du type de ressource dans « extensions AWS publiques » du AWS CloudFormation registre ou à l'aide de la commande CLI suivante :

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Pour plus d'informations, consultez la section Gestion des extensions via le AWS CloudFormation registre et la référence aux types de AWS ressources et de propriétés dans le guide de AWS CloudFormation l'utilisateur.

> **Note**
>
> Les règles proactives ne corrigent pas les ressources marquées comme NON_COMPLIANT et n'empêchent pas leur déploiement.

Évaluation de vos ressources

Pour activer l'évaluation proactive

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région qui prend en charge les AWS Config règles. Pour obtenir la liste des régions AWS prises en charge, consultez Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation de gauche, choisissez Règles. Pour obtenir la liste des règles gérées qui prennent en charge l'évaluation proactive, consultez la section Liste des règles AWS Config gérées par mode d'évaluation.
4. Choisissez une règle et l'option Modifier la règle correspondant à la règle que vous souhaitez mettre à jour.
5. Choisissez Activer l'évaluation proactive pour le Mode d'évaluation afin de pouvoir évaluer les paramètres de configuration de vos ressources avant leur déploiement.
6. Choisissez Enregistrer.

> **Note**
>
> Vous pouvez également activer l'évaluation proactive à l'aide de la `put-config-rule`commande et en activant `PROACTIVE` `EvaluationModes` ou en utilisant l'PutConfigRuleaction et en activant `PROACTIVE` pour`EvaluationModes`.

Après avoir activé l'évaluation proactive, vous pouvez utiliser l'StartResourceEvaluationAPI et l'GetResourceEvaluationSummaryAPI pour vérifier si les ressources que vous spécifiez dans ces commandes seront signalées comme NON CONFORMES par les règles proactives de votre compte dans votre région.

Par exemple, commencez par l' StartResourceEvaluation API :

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Vous devriez recevoir le `ResourceEvaluationId` dans la sortie :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Ensuite, utilisez l'API `ResourceEvaluationId` avec l' GetResourceEvaluationSummary API pour vérifier le résultat de l'évaluation :

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Votre résultat doit être similaire à ce qui suit :

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Pour obtenir des informations supplémentaires sur le résultat de l'évaluation, telles que la règle qui a marqué une ressource comme NON_COMPLIANT, utilisez l'API. GetComplianceDetailsByResource

Mode détectif

Utilisez l'évaluation détective pour évaluer les ressources déjà déployées. Ce type d'évaluation vous permet d'évaluer les paramètres de configuration de vos ressources existantes.

Évaluation de vos ressources (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une région compatible avec les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation, choisissez Règles. La page Règles indique le nom, les mesures correctives associées et l'état de conformité de chaque règle.
4. Choisissez une règle dans le tableau.
5. Dans la liste déroulante Actions, choisissez Réévaluer.
6. AWS Config commence à évaluer les ressources par rapport à votre règle.

> **Note**
>
> Vous pouvez réévaluer une règle une fois par minute. Vous devez attendre AWS Config que l'évaluation de votre règle soit terminée avant de commencer une autre évaluation. Vous ne pouvez pas exécuter une évaluation si une mise à jour ou une suppression de règle sont en cours en même temps.

Évaluation de vos ressources (CLI)

- Utilisez la commande start-config-rules-evaluation :

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config commence à évaluer les configurations de ressources enregistrées par rapport à votre règle. Vous pouvez également spécifier plusieurs règles dans votre demande :

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

Évaluation de vos ressources (API)

Utilisez l'action StartConfigRulesEvaluation.

Supprimer les résultats d'évaluation des AWS Config règles

Une fois qu'AWS Config a évalué votre règle, vous pouvez voir les résultats de l'évaluation sur la page Règles ou Rules details (Détails de la règle) pour la règle. Si les résultats de l'évaluation sont incorrects ou si vous souhaitez effectuer à nouveau l'évaluation, vous pouvez supprimer les résultats de l'évaluation actuelle pour la règle. Par exemple, si votre règle a évalué incorrectement vos ressources ou si vous avez supprimé récemment des ressources de votre compte, vous pouvez supprimer les résultats de l'évaluation, puis en exécuter une nouvelle.

Supprimer les résultats de l'évaluation (console)

1. Connectez-vous à la AWS Management Console et ouvrez la console AWS Config à l'adresse https://console.aws.amazon.com/config/.
2. Dans le AWS Management Console menu, vérifiez que le sélecteur de région est défini sur une AWS région qui prend en charge les AWS Config règles. Pour obtenir la liste des régions prises en charge, consultez la section AWS ConfigRégions et points de terminaison dans le Référence générale d'Amazon Web Services.
3. Dans le volet de navigation, sélectionnez Rules. La page Règles indique le nom, les mesures correctives associées et le statut de conformité de chaque règle.
4. Choisissez une règle dans le tableau.
5. Dans la liste déroulante Actions, choisissez Supprimer les résultats.
6. Lorsque vous y êtes invité, tapez Supprimer (cette entrée distingue les majuscules et minuscules), puis choisissez Supprimer. Une fois que vous avez supprimé une évaluation, vous ne pouvez pas la récupérer.

7. Une fois que les résultats de l'évaluation ont été supprimés, vous pouvez démarrer manuellement une nouvelle évaluation.

Suppression des résultats d'évaluation (CLI)

- Utilisez la commande delete-evaluation-results.

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

  AWS Config supprime les résultats de l'évaluation pour la règle.

Suppression des résultats d'évaluation (API)

Utilisez l'action DeleteEvaluationResults.

Gestion des AWS Config règles pour tous les comptes de votre organisation

> **Important**
>
> Les règles organisationnelles ne peuvent être créées qu'à l'aide de l'API ou de la CLI. Cette opération n'est pas prise en charge dans la AWS Config console.

AWS Config vous permet de gérer les AWS Config règles dans l'ensemble Comptes AWS d'une organisation. Vous pouvez :

- Créez, mettez à jour et supprimez des AWS Config règles centralisées pour tous les comptes de votre organisation.
- Déployez un ensemble de AWS Config règles communes à tous les comptes et spécifiez les comptes pour lesquels AWS Config les règles ne doivent pas être créées.
- Utilisez les API du compte de gestion AWS Organizations pour renforcer la gouvernance en vous assurant que les AWS Config règles sous-jacentes ne sont pas modifiables par les comptes membres de votre organisation.

Considérations

Pour les déploiements dans différentes régions

L'appel d'API pour déployer des règles et des packs de conformité entre les comptes est spécifique à AWS la région. Au niveau de l'organisation, vous devez modifier le contexte de votre appel d'API vers une autre région si vous souhaitez déployer des règles dans d'autres régions. Par exemple, pour déployer une règle dans la région USA Est (Virginie du Nord), remplacez la région par USA Est (Virginie du Nord), puis appelez `PutOrganizationConfigRule`.

Pour les comptes au sein d'une organisation

Si un nouveau compte rejoint une organisation, la règle ou le pack de conformité est déployé(e) sur ce compte. Lorsqu'un compte quitte une organisation, la règle ou le pack de conformité est supprimé(e).

Si vous déployez une règle organisationnelle ou un pack de conformité dans un compte administrateur d'organisation avant d'établir un administrateur délégué et de déployer une règle organisationnelle ou un pack de conformité dans le compte administrateur délégué, vous ne pourrez pas voir la règle organisationnelle ou le pack de conformité dans le compte administrateur de l'organisation depuis le compte administrateur délégué, ni voir la règle organisationnelle ou le pack de conformité dans le compte administrateur délégué depuis le compte administrateur de l'organisation. Les DescribeOrganizationConformancePacksAPI DescribeOrganizationConfigRuleset peuvent uniquement voir et interagir avec les ressources liées à l'organisation qui ont été déployées depuis le compte appelant ces API.

Mécanisme de nouvelle tentative pour les nouveaux comptes ajoutés à une organisation

Le déploiement des règles organisationnelles et des packs de conformité existants fera l'objet d'une nouvelle tentative uniquement dans les 7 heures suivant l'ajout d'un compte à votre organisation si aucun enregistreur n'est disponible. Vous devez créer un enregistreur s'il n'en existe pas dans les 7 heures qui suivent l'ajout d'un compte à votre organisation.

Comptes de gestion de l'organisation, administrateurs délégués et rôles liés aux services

Si vous utilisez un compte de gestion d'organisation et que vous avez l'intention de faire appel à un administrateur délégué pour le déploiement organisationnel, sachez que cela AWS Config ne créera pas automatiquement le rôle lié au service (SLR). Vous devez créer manuellement le rôle lié au service (SLR) séparément à l'aide d'IAM.

Si vous ne possédez pas de reflex pour votre compte de gestion, vous ne pourrez pas déployer de ressources vers ce compte à partir d'un compte d'administrateur délégué. Vous pourrez toujours déployer des AWS Config règles sur les comptes membres depuis les comptes de gestion et les comptes d'administrateur délégué. Pour plus d'informations, consultez la section Utilisation des rôles liés à un service dans le Guide de l'AWS Identity and Access Management utilisateur (IAM).

Déploiement

Pour plus d'informations sur la manière AWS Config d'intégrer AWS Organizations, consultez AWS Config et AWS Organizations dans le Guide de AWS Organizations l'utilisateur. Assurez-vous que AWS Config l'enregistrement est activé avant d'utiliser les API suivantes pour gérer les AWS Config règles Comptes AWS dans l'ensemble d'une organisation :

- PutOrganizationConfigRule, ajoute ou met à jour une règle de configuration organisationnelle pour l'ensemble de votre organisation en évaluant si vos AWS ressources sont conformes aux configurations souhaitées.
- DescribeOrganizationConfigRules, renvoie une liste des règles de configuration de l'organisation.
- GetOrganizationConfigRuleDetailedStatus, renvoie le statut détaillé de chaque compte membre au sein d'une organisation pour une règle de configuration d'organisation donnée.
- GetOrganizationCustomRulePolicy, renvoie la définition de politique contenant la logique de la règle de politique personnalisée de configuration de votre organisation.
- DescribeOrganizationConfigRuleStatuts, indique l'état de déploiement des règles de configuration de l'organisation pour une organisation.
- DeleteOrganizationConfigRule, supprime la règle de configuration d'organisation spécifiée et tous ses résultats d'évaluation de tous les comptes membres de cette organisation.

Prise en charge de la région

Le déploiement de AWS Config règles sur les comptes des membres d'une AWS organisation est pris en charge dans les régions suivantes.

Nom de la région	Région	Point de terminaison	Protocole	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Corriger les ressources non conformes à l'aide de règles AWS Config

AWS Config vous permet de corriger les ressources non conformes évaluées par. AWS Config Rules AWS Config applique la correction à l'aide de documents AWS Systems Manager d'automatisation. Ces documents définissent les actions à effectuer sur les AWS ressources non conformes évaluées par AWS Config Rules. Vous pouvez associer des documents SSM à l'aide de l' AWS Management Console ou des API.

AWS Config fournit un ensemble de documents d'automatisation gérés avec des actions correctives. Vous pouvez également créer et associer des documents d'automatisation personnalisés à des AWS Config règles.

Pour appliquer la correction aux ressources non conformes, vous pouvez soit choisir l'action de correction que vous souhaitez associer dans une liste préremplie, soit créer vos propres actions de correction personnalisées à l'aide de documents SSM. AWS Config fournit une liste recommandée de mesures correctives dans le AWS Management Console.

Dans le AWS Management Console, vous pouvez choisir de corriger manuellement ou automatiquement les ressources non conformes en associant des actions de correction à des règles. AWS Config Pour toutes les actions de correction, vous pouvez choisir une correction manuelle ou automatique.

Rubriques

- Prérequis
- Configuration de la correction manuelle (console)
- Configuration de la correction automatique (console)
- Suppression d'une action de correction (console)
- Gestion de correction (API)
- Prise en charge de la région

Prérequis

Avant de commencer à appliquer des corrections sur les ressources non conformes, vous devez sélectionner une règle et configurer la correction (manuelle ou automatique) pour celle-ci.

Configuration de la correction manuelle (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Règles sur la gauche, puis sur la page Règles, choisissez Ajouter une règle pour ajouter de nouvelles règles à la liste des règles

   Pour les règles existantes, sélectionnez la règle non conforme dans la liste des règles et choisissez la liste déroulante Actions.
3. Dans la liste déroulante Actions, choisissez Gérer les mesures correctives. Sélectionnez « Correction manuelle », puis choisissez la mesure corrective appropriée dans la liste recommandée.

   > **Note**
   >
   > Vous ne pouvez gérer les corrections que pour les règles non liées à AWS Config un service. Pour plus d'informations, consultez Règles AWS liées à un service.

   Selon la mesure corrective sélectionnée, vous voyez les paramètres spécifiques ou aucun paramètre.
4. (Facultatif) : si vous souhaitez transmettre l'ID de ressource des ressources non conformes à la mesure corrective, choisissez Resource ID parameter (Paramètre d'ID de ressource). Si cette

option est sélectionnée, ce paramètre est remplacé par l'ID de la ressource à corriger lors de l'exécution.

Chaque paramètre a une valeur statique ou une valeur dynamique. Si vous ne choisissez pas de paramètre d'ID de ressource spécifique dans la liste déroulante, vous pouvez saisir des valeurs pour chaque clé. Si vous choisissez un paramètre d'ID de ressource dans la liste déroulante, vous pouvez saisir des valeurs pour toutes les autres clés, à l'exception du paramètre d'ID de ressource sélectionné.

5. Choisissez Enregistrer. La page Règles s'affiche.

Pour résoudre les problèmes liés à l'échec des actions de correction, vous pouvez exécuter la AWS commande de l'interface de ligne de commande `describe-remediation-execution-status` pour obtenir une vue détaillée de l'exécution d'une correction pour un ensemble de ressources. Les détails incluent l'état, les horodatages des étapes d'exécution de correction et tous les messages d'erreur pour les étapes ayant échoué.

Configuration de la correction automatique (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Règles sur la gauche, puis sur la page Règles, choisissez Ajouter une règle pour ajouter de nouvelles règles à la liste des règles.

   Pour les règles existantes, sélectionnez la règle non conforme dans la liste des règles et choisissez la liste déroulante Actions.
3. Dans la liste déroulante Actions, choisissez Gérer les mesures correctives. Sélectionnez « Correction automatique », puis choisissez la mesure corrective appropriée dans la liste recommandée.

   > **Note**
   >
   > Vous ne pouvez gérer les corrections que pour les règles non liées à AWS Config un service. Pour plus d'informations, consultez Règles AWS liées à un service.

   Selon la mesure corrective sélectionnée, vous voyez les paramètres spécifiques ou aucun paramètre.

4. Choisissez Résolution automatique pour corriger automatiquement les ressources non conformes.

   Si une ressource n'est toujours pas conforme après la correction automatique, vous pouvez définir la règle pour réessayer la correction automatique. Saisissez les nouvelles tentatives et secondes souhaitées.

   > **Note**
   >
   > Des coûts sont associés à l'exécution multiple d'un script de correction. Les nouvelles tentatives ont lieu uniquement si la correction échoue et pendant la période spécifiée ; par exemple, 5 tentatives en 300 secondes.

5. (Facultatif) : si vous souhaitez transmettre l'ID de ressource des ressources non conformes à la mesure corrective, choisissez Resource ID parameter (Paramètre d'ID de ressource). Si cette option est sélectionnée, ce paramètre est remplacé par l'ID de la ressource à corriger lors de l'exécution.

   Chaque paramètre a une valeur statique ou une valeur dynamique. Si vous ne choisissez pas de paramètre d'ID de ressource spécifique dans la liste déroulante, vous pouvez saisir des valeurs pour chaque clé. Si vous choisissez un paramètre d'ID de ressource dans la liste déroulante, vous pouvez saisir des valeurs pour toutes les autres clés, à l'exception du paramètre d'ID de ressource sélectionné.

6. Choisissez Enregistrer. La page Règles s'affiche.

Pour résoudre les problèmes liés à l'échec des actions de correction

Pour résoudre les problèmes liés à l'échec des actions de correction, vous pouvez exécuter la AWS commande de l'interface de ligne de commande `describe-remediation-execution-status` pour obtenir une vue détaillée de l'exécution d'une correction pour un ensemble de ressources. Les détails incluent l'état, les horodatages des étapes d'exécution de correction et tous les messages d'erreur pour les étapes ayant échoué.

La correction automatique peut être initiée même pour les ressources conformes

Si vous activez la correction automatique pour une AWS Config règle spécifique à l'aide de l'API PutRemediationConfigurations ou de la AWS Config console, cela lance le processus de correction pour toutes les ressources non conformes à cette règle spécifique. Le processus de correction

automatique repose sur l'instantané des données de conformité qui est capturé périodiquement. Toute ressource non conforme mise à jour entre le calendrier des instantanés continuera d'être corrigée sur la base du dernier instantané de données de conformité connu.

Cela signifie que dans certains cas, la correction automatique peut être initiée même pour les ressources conformes, étant donné que le processeur bootstrap utilise une base de données dont les résultats d'évaluation peuvent être périmés sur la base du dernier instantané de données de conformité connu.

Suppression d'une action de correction (console)

Pour supprimer une règle, vous devez d'abord supprimer l'action de correction associée à cette règle.

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Règles sur la gauche, puis sur la page Règles, sélectionnez la règle à partir de la liste des règles et choisissez Afficher les détails.
3. Sur la page *Nom de la règle*, accédez à la section Mesure corrective. Développez la section pour afficher des informations supplémentaires.
4. Dans la section Mesure corrective, choisissez Supprimer et confirmez votre action de suppression.

   > **Note**
   >
   > Si la correction est en cours, la mesure corrective n'est pas supprimée. Si vous choisissez Supprimer une mesure corrective, vous ne pouvez pas récupérer la mesure corrective. La suppression d'une mesure corrective ne supprime pas la règle associée.

   Si une mesure corrective est supprimée, le paramètre ID de ressource sera vide et affichera N/A. Sur la page Règles, la colonne de la mesure corrective indique Non défini pour la règle associée.

Gestion de correction (API)

Correction manuelle

Utilisez les actions AWS Config d'API suivantes pour gérer les mesures correctives :

- DeleteRemediationConfiguration, supprime la configuration de correction.
- DescribeRemediationConfigurations, renvoie les détails d'une ou de plusieurs configurations de correction.
- DescribeRemediationExecutionStatus, fournit une vue détaillée de l'exécution d'une correction pour un ensemble de ressources, y compris l'état, les horodatages indiquant le moment où les étapes de l'exécution de la correction ont lieu et les éventuels messages d'erreur relatifs aux étapes ayant échoué.
- PutRemediationConfigure, ajoute ou met à jour la configuration de correction avec une AWS Config règle spécifique avec la cible ou l'action sélectionnée.
- StartRemediationExécution : exécute une correction à la demande pour les AWS Config règles spécifiées par rapport à la dernière configuration de correction connue.

Correction automatique

Utilisez les actions AWS Config d'API suivantes pour gérer la correction automatique :

- PutRemediationExceptions, ajoute une nouvelle exception ou met à jour une exception existante pour une ressource spécifique avec une règle spécifique AWS Config .
- DescribeRemediationExceptions : renvoie les détails d'une ou de plusieurs exceptions de correction.
- DeleteRemediationExceptions : supprime une ou plusieurs exceptions de correction mentionnées dans les clés de ressource.

Prise en charge de la région

Actuellement, les mesures correctives AWS Config relatives aux règles sont prises en charge dans les régions suivantes :

Nom de la région	Région	Point de terminaison	Protocole	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrique (Le Cap)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asie-Pacifique (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada Ouest (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Espagne)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israël (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Moyen-Orient (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Résolution des problèmes

Vérifiez les problèmes suivants pour les résoudre si vous ne parvenez pas à supprimer une AWS Config règle ou si vous recevez un message d'erreur similaire à ce qui suit : « Une erreur s'est produite avec AWS Config ».

L'entité AWS Identity and Access Management (IAM) dispose d'autorisations pour l'API DeleteConfigRule

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Utilisateurs ou Rôles.
3. Choisissez l'utilisateur ou le rôle que vous avez utilisé pour supprimer la AWS Config règle, puis développez les politiques d'autorisations.
4. Dans l'onglet Autorisations, choisissez JSON.
5. Dans le volet d'aperçu JSON, vérifiez que la politique IAM autorise les autorisations pour l'API DeleteConfigRule.

La limite d'autorisation de l'entité IAM autorise l'API DeleteConfigRule

Si l'entité IAM possède une limite d'autorisations, assurez-vous qu'elle autorise les autorisations pour l' DeleteConfigRule API.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Utilisateurs ou Rôles.
3. Choisissez l'utilisateur ou le rôle que vous avez utilisé pour supprimer la AWS Config règle, étendez la limite des autorisations, puis choisissez JSON.
4. Dans le volet d'aperçu JSON, vérifiez que la politique IAM autorise les autorisations pour l'API DeleteConfigRule.

> **Warning**
>
> Les utilisateurs IAM disposent d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de n'octroyer à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces utilisateurs lorsqu'ils ne sont plus nécessaires.

La politique de contrôle des services (SCP) autorise l'API DeleteConfigRule

1. Ouvrez la AWS Organizations console à l'adresse https://console.aws.amazon.com/organizations/ à l'aide du compte de gestion de l'organisation.
2. Dans Nom du compte, choisissez le Compte AWS.
3. Dans Politiques, développez les politiques de contrôle des services et notez les politiques SCP associées.
4. En haut de la page, sélectionnez Politiques.
5. Sélectionnez la politique, puis choisissez Afficher les détails.
6. Dans le volet d'aperçu JSON, vérifiez que la politique autorise l'API DeleteConfigRule.

La règle n'est pas une règle liée à un service

Lorsque vous activez une norme de sécurité, elle AWS Security Hub crée des règles liées au service pour vous. Vous ne pouvez pas supprimer ces règles liées aux services à l'aide de AWS Config, et le bouton de suppression est grisé. Pour supprimer une règle liée à un service, consultez la section Désactivation d'une norme de sécurité dans le Guide de l'utilisateur du Security Hub.

Aucune action corrective n'est en cours

Vous ne pouvez pas supprimer AWS Config les règles qui comportent des actions de correction en cours. Suivez les étapes pour supprimer l'action de correction associée à cette règle. Réessayez ensuite de supprimer la règle.

> **Important**
>
> Supprimez uniquement les actions de correction dont l'état a échoué ou réussi.

Packs de conformité

Un pack de conformité est un ensemble de AWS Config règles et d'actions correctives qui peuvent être facilement déployées en tant qu'entité unique dans un compte et une région ou au sein d'une organisation dans. AWS Organizations

Les packs de conformité sont créés au moyen d'un modèle YAML qui contient la liste des règles gérées ou personnalisées et des actions de correction AWS Config . Vous pouvez également utiliser AWS Systems Manager des documents (documents SSM) pour stocker vos modèles de packs de conformité AWS et les déployer directement à l'aide des noms de documents SSM. Vous pouvez déployer le modèle à l'aide de la console AWS Config ou de la AWS CLI.

Pour démarrer rapidement et évaluer votre AWS environnement, utilisez l'un des exemples de modèles de pack de conformité. Vous pouvez également créer un fichier YAML de pack de conformité à partir de zéro sur la base du pack de conformité personnalisé.

Rubriques

- Prérequis
- Prise en charge de la région
- AWS Config Contrôles de processus dans le cadre d'un pack de conformité
- Exemples de modèles de pack de conformité
- Packs de conformité personnalisés
- Affichage des données de conformité dans le tableau de bord des packs de conformité
- Affichage de la chronologie de l'historique de conformité des packs de conformité
- Déploiement d'un pack de conformité à l'aide de la console AWS Config
- Déploiement d'un pack de conformité à l'aide de l' AWS Command Line Interface
- Gestion des packs de conformité (API)
- Gestion des packs de conformité dans tous les comptes de votre organisation
- Résolution des problèmes

Prérequis

Avant de déployer votre pack de conformité, activez l' AWS Config enregistrement.

Commencer AWS Config l'enregistrement

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Pour démarrer l'enregistrement, sous Recording is off (L'enregistrement est désactivé), choisissez Turn on (Activer). À l'invite, choisissez Continuer.

Conditions préalables à l'utilisation d'un pack de conformité avec la correction

Avant de déployer des packs de conformité à l'aide d'exemples de modèles avec correction, vous devez créer des ressources appropriées telles que l'automatisation assume le rôle et d'autres AWS ressources en fonction de votre objectif de correction.

Si vous disposez d'un rôle d'automatisation existant que vous utilisez pour la correction à l'aide de documents SSM, vous pouvez directement fournir l'ARN de ce rôle. Si vous disposez de ressources, vous pouvez les fournir dans le modèle.

> **Note**
>
> Lors du déploiement d'un pack de conformité avec la correction dans une organisation, l'ID du compte de gestion de l'organisation doit être spécifié. Dans le cas contraire, lors du déploiement du pack de conformité de l'organisation, AWS Config remplace automatiquement l'ID du compte de gestion par l'ID du compte membre.

AWS Config ne prend pas en charge les fonctions AWS CloudFormation intrinsèques pour le rôle d'exécution de l'automatisation. Vous devez fournir l'ARN exact du rôle sous forme de chaîne.

Pour de plus amples informations sur la façon de transmettre l'ARN exact, veuillez consulter Exemples de modèles de pack de conformité. Lors de l'utilisation d'exemples de modèles, mettez à jour votre ID de compte et votre ID de compte de gestion pour l'organisation.

Conditions préalables à l'utilisation d'un pack de conformité avec une ou plusieurs règles AWS Config

Avant de déployer un pack de conformité avec une ou plusieurs AWS Config règles personnalisées, créez les ressources appropriées telles que la AWS Lambda fonction et le rôle d'exécution correspondant.

Si vous avez une AWS Config règle personnalisée existante, vous pouvez directement fournir la AWS Lambda fonction ARN of pour créer une autre instance de cette règle personnalisée dans le cadre du pack.

Si aucune AWS Config règle personnalisée n'existe, vous pouvez créer une AWS Lambda fonction et utiliser l'ARN de la fonction Lambda. Pour plus d'informations, consultez AWS Config Règles personnalisées.

Si votre AWS Lambda fonction est présente dans un autre Compte AWS, vous pouvez créer des AWS Config règles avec l'autorisation appropriée pour les AWS Lambda fonctions inter-comptes. Pour plus d'informations, consultez Comment gérer de manière centralisée les AWS Config règles sur plusieurs Comptes AWS articles de blog.

Same account bucket policy

AWS Config Pour pouvoir stocker les artefacts du pack de conformité, vous devez fournir un compartiment Amazon S3 et ajouter les autorisations suivantes. Pour plus d'informations sur les noms de compartiment, consultez Règles de dénomination de compartiment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
```

```
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

AWS Config Pour pouvoir stocker les artefacts du pack de conformité, vous devez fournir un compartiment Amazon S3 et ajouter les autorisations suivantes. Pour plus d'informations sur les noms de compartiment, consultez Règles de dénomination de compartiment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
```

```
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> Lors du déploiement de packs de conformité entre comptes, le nom du compartiment de diffusion Amazon S3 doit commencer par `awsconfigconforms`.

Conditions préalables pour les packs de conformité d'organisation

Spécifiez un ARN de rôle d'exécution d'automatisation pour cette correction dans le modèle, si le modèle d'entrée possède une configuration de correction automatique. Vérifiez qu'un rôle portant le nom spécifié existe dans tous les comptes (gestion et membres) d'une organisation. Vous devez créer ce rôle dans tous les comptes avant d'appeler `PutOrganizationConformancePack`. Vous pouvez créer ce rôle manuellement ou utiliser les AWS CloudFormation stack-sets pour créer ce rôle dans chaque compte.

Si votre modèle utilise une fonction AWS CloudFormation intrinsèque `Fn::ImportValue` pour importer une variable particulière, cette variable doit être définie comme un `Export Value` dans tous les comptes membres de cette organisation.

Pour les AWS Config règles personnalisées, consultez Comment gérer de manière centralisée AWS Config les règles sur plusieurs Comptes AWS blogs pour configurer les autorisations appropriées.

Politique de compartiments d'organisation :

AWS Config Pour pouvoir stocker les artefacts du pack de conformité, vous devez fournir un compartiment Amazon S3 et ajouter les autorisations suivantes. Pour plus d'informations sur les noms de compartiment, consultez Règles de dénomination de compartiment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
```

```
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> Lorsque vous déployez des packs de conformité dans une organisation, le nom du compartiment de diffusion Amazon S3 doit commencer par `awsconfigconforms`.

Prise en charge de la région

Les packs de conformité sont pris en charge dans les régions ci-dessous.

Nom de la région	Région	Point de terminaison	Protocole
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Le déploiement de packs de conformité sur les comptes membres d'une AWS organisation est pris en charge dans les régions suivantes.

Nom de la région	Région	Point de terminaison	Protocole
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Contrôles de processus dans le cadre d'un pack de conformité

Les contrôles de processus sont un type de AWS Config règle qui vous permet de suivre vos tâches externes et internes qui nécessitent une vérification dans le cadre des packs de conformité. Ces vérifications peuvent être ajoutées à un pack de conformité existant ou à un nouveau pack de conformité. Vous pouvez suivre l'ensemble de la conformité, y compris AWS Config les durées et les contrôles manuels, en un seul endroit.

Les vérifications des processus vous permettent de répertorier la conformité des exigences et des actions en un seul endroit. Ces vérifications des processus permettent d'augmenter la couverture des packs de conformité basés sur des régimes de conformité. Vous pouvez étendre le pack de conformité en ajoutant de nouvelles vérifications de processus qui suivent les processus et les actions nécessitant une vérification et un suivi manuels. Cela permet au pack de conformité de devenir le modèle fournissant des détails sur les AWS Config durées et les processus manuels d'un régime de conformité.

Vous pouvez suivre et gérer la conformité des processus qui ne sont pas associés à des modifications de configuration des ressources au sein d'un pack de conformité sous forme de vérifications des processus. Par exemple, vous pouvez ajouter une vérification de processus pour suivre l'exigence de conformité à la norme PCI-DSS, qui consiste à stocker la sauvegarde multimédia dans un emplacement hors site. Vous évaluerez manuellement la conformité de ce processus selon les directives PCI-DSS ou selon les directives de votre organisation.

Disponibilité régionale : les contrôles de processus avec les packs de conformité sont disponibles dans tous les pays Régions AWS où des packs de AWS Config conformité sont disponibles. Pour plus d’informations, consultez Prise en charge de la région.

Rubriques

- Exemple de modèle de pack de conformité pour créer des vérifications de processus
- Comprend Process Checks Within a Conformance Pack
- Modifier le statut de conformité d'une vérification de processus
- Afficher et modifier la vérification du processus (Console)

Exemple de modèle de pack de conformité pour créer des vérifications de processus

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
```

```
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

Consultez deux exemples de modèles, le modèle Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 1 et le modèle Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 2 .

Comprend Process Checks Within a Conformance Pack

1. Ajoutez une vérification de processus dans le modèle de pack de conformité. Reportez-vous à l'exemple de modèle précédent.

```
Resources:
  ConfigEnabledAllRegions:
    Properties:
      ConfigRuleName: Config-Enabled-All-Regions
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. Saisissez le nom de la vérification de processus.
3. Saisissez la description de la vérification de processus.
4. Déployez le pack de conformité depuis la Console de gestion AWS. Pour plus d'informations, consultez Déploiement d'un pack de conformité à l'aide de la console AWS Config.

> **Note**
>
> Vous pouvez également déployer les packs de conformité à l'aide de l'interface de ligne de commande (AWS CLI). Pour plus d'informations, consultez Déploiement d'un pack de conformité à l'aide de l' AWS Command Line Interface.

Modifier le statut de conformité d'une vérification de processus

Modifier le statut de conformité d'une vérification de processus (Console)

Pour modifier l'état de conformité d'un contrôle de processus (console)

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Accédez à la page AWS Config Règles.
3. Choisissez le nom de la vérification de processus que vous avez spécifié dans le modèle, ainsi que l'identifiant, dans le pack de conformité.

   > **Note**
   >
   > Toutes les vérifications de processus du même pack de conformité ont le même suffixe.

4. Sur la page Détails de la règle, vous ne pouvez pas modifier la règle, mais vous pouvez modifier sa conformité. Dans la section Conformité manuelle, choisissez Modifier la conformité.
5. Choisissez la conformité appropriée dans la liste déroulante.
6. (Facultatif) Saisissez une description pour le statut de conformité.
7. Choisissez Enregistrer.

Modifier le statut de conformité d'une vérification de processus (CLI)

Pour modifier l'état de conformité d'une vérification de processus (CLI)

Vous pouvez mettre à jour la conformité des vérifications de processus au sein d'un pack de conformité à l'aide de l'interface de ligne de commande AWS (AWS CLI).

Pour l'installer AWS CLI sur votre machine locale, consultez la section Installation de l'interface de ligne de commande AWS dans le guide de AWS CLI l'utilisateur.

Si nécessaire, saisissez `AWS Config ure` pour configurer le AWS CLI afin d'utiliser une AWS région dans laquelle des packs de AWS Config conformité sont disponibles.

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez la commande suivante pour mettre à jour la conformité d'un processus, vérifiez où se `ComplianceResourceId` trouve votre`Account ID`, et incluez le nom de votre règle.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Appuyez sur Entrée pour exécuter la commande.

Modifier le statut de conformité d'une vérification de processus (API)

Pour modifier l'état de conformité d'une vérification de processus (API)

Une fois le déploiement terminé, pour mettre à jour les évaluations et la conformité des vérifications de processus, utilisez l'API `PutExternalEvaluation`. Pour plus d'informations, consultez la section PutExternalÉvaluation.

Afficher et modifier la vérification du processus (Console)

Vous ne pouvez afficher les vérifications de processus que lorsqu'un état de conformité a été ajouté aux vérifications de processus. Sélectionnez le pack de conformité spécifique pour afficher toutes les vérifications de processus dans ce pack de conformité. Vous pouvez voir ici une liste des contrôles de processus conformes et non conformes.

Comme il s'agit d'une règle liée à un service, vous ne pouvez pas modifier la vérification du processus à partir de la page Détails de la règle.

> **Note**
>
> Toutefois, vous pouvez mettre à jour la conformité du contrôle de processus en choisissant Modifier la conformité et en sélectionnant la valeur appropriée parmi Conforme, Non conforme ou Non applicable.

Vous pouvez modifier ou supprimer une vérification de processus depuis le pack de conformité dans lequel vous avez ajouté les vérifications de processus.

Exemples de modèles de pack de conformité

Voici les modèles YAML du pack de conformité que vous pouvez voir dans AWS Config la console. Dans chaque modèle de pack de conformité, vous pouvez utiliser une ou plusieurs règles et actions

de correction AWS Config. Les règles AWS Config répertoriées dans le pack de conformité peuvent être des règles AWS Config gérées et/ou des règles AWS Config personnalisées. Vous pouvez télécharger tous les modèles de packs de conformité depuis GitHub.

> **Important**
>
> Les packs de conformité fournissent un cadre général de conformité pour vous aider à créer des contrôles de gouvernance de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de règles AWS Config gérées ou personnalisées et d'actions de correction AWS Config. Les exemples de modèle de pack de conformité AWS visent à vous aider à créer vos propres packs de conformité avec des règles, des paramètres d'entrée et des actions de correction différents ou supplémentaires adaptés à votre environnement. Les exemples de modèle, y compris ceux liés aux normes de conformité et aux référence du secteur, ne sont pas conçus pour assurer votre conformité à une norme de gouvernance spécifique. Ils ne peuvent ni remplacer vos efforts internes ni garantir que vous réussirez une évaluation de conformité.

> **Note**
>
> Il est recommandé de consulter les règles disponibles dans la région où vous déployez un pack de conformité (liste des règles AWS Config gérées par disponibilité régionale) et de modifier le modèle pour les règles qui ne sont pas encore disponibles dans cette région avant le déploiement.

Rubriques

- AWSPack de conformité pour garde-corps Control Tower Detective
- Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Material
- Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Standard
- Bonnes pratiques de fonctionnement pour ACSC Essentials 8
- Bonnes pratiques de fonctionnement pour ACSC ISM
- Bonnes pratiques de fonctionnement pour l'IA et le ML
- Bonnes pratiques de fonctionnement pour Amazon API Gateway
- Bonnes pratiques opérationnelles pour Amazon CloudWatch
- Bonnes pratiques opérationnelles pour Amazon DynamoDB

- Bonnes pratiques opérationnelles pour Amazon S3
- Bonnes pratiques de fonctionnement pour APRA CPG 234
- Bonnes pratiques de fonctionnement pour la gestion des ressources
- Bonnes pratiques de fonctionnement pour AWS Backup
- Bonnes pratiques opérationnelles pour la gestion des AWS identités et des accès
- Meilleures pratiques opérationnelles pour le pilier de fiabilité du AWS framework Well-Architected
- Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected
- Bonnes pratiques de fonctionnement pour le BCP et la DR
- Bonnes pratiques de fonctionnement pour BNM RMiT
- Bonnes pratiques de fonctionnement pour le profil moyen de contrôle du cloud du Canadian Centre for Cyber Security (CCCS)
- Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 1
- Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 2
- Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG1
- Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG2
- Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG3
- Bonnes pratiques de fonctionnement pour CIS Top 20
- Bonnes pratiques de fonctionnement pour CISA Cyber Essentials
- Bonnes pratiques de fonctionnement pour la division Criminal Justice Information Services (CJIS)
- Bonnes pratiques de fonctionnement pour CMMC niveau 1
- Bonnes pratiques de fonctionnement pour CMMC niveau 2
- Bonnes pratiques de fonctionnement pour CMMC niveau 3
- Bonnes pratiques de fonctionnement pour CMMC niveau 4
- Bonnes pratiques de fonctionnement pour CMMC niveau 5
- Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 1
- Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 2
- Bonnes pratiques de fonctionnement pour les services de calcul
- Bonnes pratiques de fonctionnement pour la résilience des données
- Bonnes pratiques de fonctionnement pour les services de base de données
- Bonnes pratiques de fonctionnement pour les services de lac de données et d'analyse
- Bonnes pratiques de fonctionnement pour DevOps

- Bonnes pratiques de fonctionnement pour EC2
- Bonnes pratiques de fonctionnement pour les services de chiffrement et de gestion des clés
- Bonnes pratiques de fonctionnement pour le guide de la cybersécurité pour les PME de l'ENISA
- Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau faible)
- Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau modéré)
- Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau élevé)
- Bonnes pratiques de fonctionnement pour la norme FDA CFR Titre 21 Partie 11
- Bonnes pratiques de fonctionnement pour FedRAMP(Low)
- Bonnes pratiques de fonctionnement pour FedRAMP (modérée)
- Bonnes pratiques de fonctionnement pour FFIEC
- Bonnes pratiques de fonctionnement pour Germany Cloud Computing Compliance Criteria Catalog (C5)
- Bonnes pratiques de fonctionnement pour Gramm Leach Bliley Act (GLBA)
- Bonnes pratiques de fonctionnement pour GxP EU Annex 11
- Bonnes pratiques de fonctionnement pour la sécurité HIPAA
- Bonnes pratiques de fonctionnement pour IRS 1#075
- Bonnes pratiques de fonctionnement pour K-ISMS
- Bonnes pratiques de fonctionnement pour l'équilibrage de charge
- Bonnes pratiques de fonctionnement pour la journalisation
- Bonnes pratiques de fonctionnement pour les services de gestion et de gouvernance
- Bonnes pratiques de fonctionnement pour MAS Notice 655
- Bonnes pratiques de fonctionnement pour MAS TRMG
- Bonnes pratiques de fonctionnement pour la surveillance
- Bonnes pratiques de fonctionnement pour NBC TRMG
- Bonnes pratiques de fonctionnement pour NERC CIP BCSI
- Bonnes pratiques de fonctionnement pour les principes de sécurité du cloud NCSC
- Bonnes pratiques de fonctionnement pour NCSC Cyber Assesment Framework
- Bonnes pratiques de fonctionnement pour les services de mise en réseau et de diffusion de contenu
- Bonnes pratiques de fonctionnement pour NIST 800-53 rev 4
- Bonnes pratiques de fonctionnement pour NIST 800-53 rev 5

- Bonnes pratiques de fonctionnement pour NIST 800 171
- Bonnes pratiques de fonctionnement pour NIST 800 172
- Bonnes pratiques de fonctionnement pour NIST 800 181
- Bonnes pratiques de fonctionnement pour NIST 1800 25
- Bonnes pratiques de fonctionnement pour NIST CSF
- Bonnes pratiques de fonctionnement pour le cadre de confidentialité NIST v1.0
- Bonnes pratiques de fonctionnement pour NYDFS 23
- Bonnes pratiques de fonctionnement pour NZISM
- Bonnes pratiques de fonctionnement pour PCI DSS 3.2.1
- Bonnes pratiques de fonctionnement pour les ressources accessibles au public
- Bonnes pratiques de fonctionnement pour le cadre de cybersécurité RBI pour les UCB
- Bonnes pratiques de fonctionnement pour RBI MD-ITF
- Bonnes pratiques de fonctionnement pour les services de sécurité, d'identité et de conformité
- Bonnes pratiques de fonctionnement pour le sans serveur
- Bonnes pratiques de fonctionnement pour les services de stockage
- Bonnes pratiques de fonctionnement pour SWIFT CSP
- Bonnes pratiques de sécurité pour Amazon Elastic Container Service (Amazon ECS)
- Bonnes pratiques de sécurité pour Amazon Elastic File System (Amazon EFS)
- Bonnes pratiques de sécurité pour Amazon Elastic Kubernetes Service (Amazon EKS)
- Bonnes pratiques en matière de sécurité pour Amazon CloudFront
- Bonnes pratiques en matière de sécurité pour Amazon OpenSearch Service
- Bonnes pratiques de sécurité pour Amazon Redshift
- Bonnes pratiques de sécurité pour Amazon Relational Database Service (Amazon RDS)
- Bonnes pratiques de sécurité pour AWS Auto Scaling
- Bonnes pratiques de sécurité pour AWS CloudTrail
- Bonnes pratiques de sécurité pour AWS CodeBuild
- Bonnes pratiques de sécurité pour Amazon ECR
- Bonnes pratiques de sécurité pour AWS Lambda
- Bonnes pratiques de sécurité pour AWS Network Firewall
- Bonnes pratiques en matière de sécurité pour Amazon SageMaker

- Bonnes pratiques de sécurité pour AWS Secrets Manager
- Bonnes pratiques de sécurité pour AWS WAF
- Exemples de modèle avec action de correction

AWSPack de conformité pour garde-corps Control Tower Detective

Le modèle est disponible sur GitHub : AWSControl Tower Detective Guardrails Conformance Pack.

Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Material

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Guide de mise en œuvre du cloud computing ABS 2.0 - Material Workloads et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles du guide d'implémentation de l'ABS Cloud Computing. Un contrôle du guide d'implémentation du cloud computing ABS peut être lié à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et

ID du contrôle	AWS Règle de configuration	Conseils
		de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
section4a-govern-the-cloud-2-material-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-3-material-workloads	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4a-govern-the-cloud-3-material-workloads	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.
section4a-govern-the-cloud-3-standard-workloads	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure -the-cloud-1-standard-workl oads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-material-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
section4b-design-and-secure-the-cloud-3-material-workloads	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-material-workloads	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
section4b-design-and-secure-the-cloud-3-material-workloads	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-material-workloads	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-material-workloads	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.
section4b-design-and-secure-the-cloud-4-material-workloads	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
section4b-design-and-secure-the-cloud-4-material-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-material-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
section4b-design-and-secure-the-cloud-4-material-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-material-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-4-material-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.
section4b-design-and-secure-the-cloud-4-material-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-material-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure -the-cloud-4-standard-workl oads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
section4b-design-and-secure-the-cloud-5-material-workloads	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
section4b-design-and-secure-the-cloud-5-material-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-material-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
section4b-design-and-secure-the-cloud-5-material-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-material-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
section4b-design-and-secure-the-cloud-6-material-workloads	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-material-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-material-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-material-workloads	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-material-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
section4b-design-and-secure-the-cloud-8-material-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-material-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure -the-cloud-8-standard-workl oads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
section4b-design-and-secure-the-cloud-9-material-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
section4b-design-and-secure-the-cloud-9-material-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-material-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
section4b-design-and-secure-the-cloud-9-material-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsageAge (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4b-design-and-secure-the-cloud-10-material-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
section4b-design-and-secure-the-cloud-10-material-workloads	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-10-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure -the-cloud-10-material-work loads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
section4b-design-and-secure-the-cloud-10-material-workloads	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
section4b-design-and-secure-the-cloud-10-material-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-10-material-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-10-material-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.
section4b-design-and-secure-the-cloud-10-material-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-material-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsageAge (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
section4b-design-and-secure-the-cloud-11-material-workloads	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L’alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l’expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
section4b-design-and-secure-the-cloud-11-material-workloads	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
section4b-design-and-secure-the-cloud-11-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-11-material-workloads	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4b-design-and-secure-the-cloud-11-material-workloads	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-11-material-workloads	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-material-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
section4b-design-and-secure-the-cloud-14-material-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-material-workloads	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
section4b-design-and-secure-the-cloud-14-material-workloads	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-material-workloads	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.
section4b-design-and-secure-the-cloud-14-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-material-workloads	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-material-workloads	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-material-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
section4b-design-and-secure-the-cloud-15-material-workloads	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-material-workloads	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-material-workloads	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-material-workloads	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que les clés principales du client (CMK) nécessaires ne sont pas programmées pour être supprimées dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
section4c-run-the-cloud-2-material-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-material-workloads	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-4-material-workloads	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.
section4c-run-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-4-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
section4c-run-the-cloud-4-material-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-material-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
section4c-run-the-cloud-6-material-workloads	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les charges de travail matérielles ABS CCIG 2.0.

Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Standard

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Guide de mise en œuvre du cloud computing ABS 2.0 - Standard Workloads et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles du guide d'implémentation de l'ABS Cloud Computing. Un contrôle du guide d'implémentation du cloud computing ABS peut être lié à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrai

ID du contrôle	AWS Règle de configuration	Conseils
		l l'activation dans plusieurs régions.
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.
section4a-govern-the-cloud-3-standard-workloads	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure -the-cloud-1-standard-workl oads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure -the-cloud-8-standard-workl oads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsageAge (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
section4b-design-and-secure-the-cloud-12-standard-workloads	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-15-standard-workloads	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
section4c-run-the-cloud-3-standard-workloads	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable.
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les charges de travail standard ABS CCIG 2.0.

Bonnes pratiques de fonctionnement pour ACSC Essentials 8

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le modèle de maturité Essential Eight du Centre australien de cybersécurité (ACSC) et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles ACSC Essential Eight. Un contrôle ACSC Essential Eight peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages. Certains des mappages vers les règles de configuration concernent la

section d'ordre supérieur (par exemple les politiques d'atténuation permettant de limiter l'impact des incidents de cybersécurité) par opposition aux sections plus prescriptives.

Cet exemple de modèle de pack de conformité contient des mappages vers les contrôles ACSC Essential 8, créé par le Commonwealth d'Australie et disponible sur ACSC | Essential Eight. La licence du cadre en vertu de la Licence publique internationale Creative Commons Attribution 4.0 et les informations sur les droits d'auteur du cadre (y compris une exclusion de garanties) sont disponibles sur ACSC | Droit d'auteur.

ID du contrôle	AWS Règle de configuration	Conseils
Application_control	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.
Application_control	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une

ID du contrôle	AWS Règle de configuration	Conseils
		liste ACL Web WAF pour la protéger contre les attaques malveillantes
Application_control	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
Application_control	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.
Application_control	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.

ID du contrôle	AWS Règle de configuration	Conseils
Application_control	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.
Application_control	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Patch_applications	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
Patch_applications	ec2-instance-managed-by-sys tems-manager	Un inventaire des plateform es logicielles et des applicati ons au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploit ation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Patch_applications	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateform e AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.
Patch_applications	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
Patch_applications	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.
Patch_applications	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Patch_applications	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Restrict_administrative_privileges	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).
Restrict_administrative_privileges	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
Restrict_administrative_privileges	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.
Restrict_administrative_privileges	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	rds-instance-iam-authentication-enabled	Assurez-vous qu'une authentification AWS Identity and Access Management (IAM) est activée sur les instances Amazon Relational Database Service (Amazon RDS) afin de contrôler l'accès aux systèmes et aux actifs. Cela permet de chiffrer le trafic réseau à destination et en provenance de la base de données au moyen du protocole SSL. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe.
Restrict_administrative_privileges	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Patch_operating_systems	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
Multi-factor_authentication	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Multi-factor_authentication	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
Multi-factor_authentication	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Multi-factor_authentication	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
Multi-factor_authentication	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
Regular_backups	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.
Regular_backups	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
Regular_backups	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.
Regular_backups	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Regular_backups	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for ACSC Essential 8.

Bonnes pratiques de fonctionnement pour ACSC ISM

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le manuel de sécurité de l'information (ISM) 2020-06 du Centre australien de cybersécurité (ACSC) et les règles de AWS configuration gérées. Chaque règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs

contrôles ISM. Un contrôle ISM peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages vers les contrôles du cadre ISM, qui a été créé par le Commonwealth d'Australie et peut être consulté dans le Manuel de sécurité des informations du gouvernement australien. La licence du cadre en vertu de la Licence publique internationale Creative Commons Attribution 4.0 et les informations sur les droits d'auteur du cadre (y compris une exclusion de garanties) sont disponibles sur ACSC | Droit d'auteur.

ID du contrôle	AWS Règle de configuration	Conseils
43	response-plan-exists-maintained (vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable.
252	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
261	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
261	elb-logging-enabled	L'activité Elastic Load Balancing est un point de

ID du contrôle	AWS Règle de configuration	Conseils
		communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
261	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
298	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
298	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
298	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
298	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
380	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.
459	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
459	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
459	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
459	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
459	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
459	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
459	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
459	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
459	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
459	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
459	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
459	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
459	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
459	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
459	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	AWS Règle de configuration	Conseils
459	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
459	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
459	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
459	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
459	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
580	audit-log-policy-exists (vérifica tion du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisation en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.

ID du contrôle	AWS Règle de configuration	Conseils
634	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.
859	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstit ution et l'identification des événements potentiellement malveillants.

ID du contrôle	AWS Règle de configuration	Conseils
974	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
974	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1139	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classique s utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociati on SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociati on SSL assurent la compatibi lité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfini e pour vos écouteurs SSL. La politique de sécurité par défaut est la suivante : ELB SecurityP olicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisat ion

ID du contrôle	AWS Règle de configuration	Conseils
1173	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1173	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
1173	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
1173	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
1173	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1228	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
1240	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1240	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
1271	rds-instance-public-access-check	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
1271	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionn alités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.
1277	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
1277	rds-instance-iam-authentication-enabled	Assurez-vous qu'une authentification AWS Identity and Access Management (IAM) est activée sur les instances Amazon Relational Database Service (Amazon RDS) afin de contrôler l'accès aux systèmes et aux actifs. Cela permet de chiffrer le trafic réseau à destination et en provenance de la base de données au moyen du protocole SSL. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe.
1277	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
1380	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
1380	ec2-instance-managed-by-sys tems-manager	Un inventaire des plateform es logicielles et des applicati ons au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploit ation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1380	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateform e AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.
1380	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
1380	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.
1380	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1380	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1380	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
1380	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
1380	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.

ID du contrôle	AWS Règle de configuration	Conseils
1380	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).
1380	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
1380	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	AWS Règle de configuration	Conseils
1380	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisate urs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opération s du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.
1380	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisate urs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
1380	rds-instance-iam-authentication-enabled	Assurez-vous qu'une authentification AWS Identity and Access Management (IAM) est activée sur les instances Amazon Relational Database Service (Amazon RDS) afin de contrôler l'accès aux systèmes et aux actifs. Cela permet de chiffrer le trafic réseau à destination et en provenance de la base de données au moyen du protocole SSL. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe.
1380	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
1380	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
1380	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
1380	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisate ur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommand e d'utiliser des politiques gérées plutôt que des politique s intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedAc tionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decry pt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1380	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
1388	restricted-common-ports	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confident ialité des systèmes. Cette règle vous permet éventuell ement de définir les paramètre s blockedPort1 à blockedPo rt5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1388	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
1401	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
1401	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
1401	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1401	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1401	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1402	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
1404	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1405	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
1405	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD_TRAIL_ENABLED

ID du contrôle	AWS Règle de configuration	Conseils
1405	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
1405	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1405	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
1405	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
1405	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
1405	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1405	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
1405	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
1405	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
1405	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
1405	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.
1405	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.
1405	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	AWS Règle de configuration	Conseils
1405	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1490	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1490	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
1490	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.
1490	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.

ID du contrôle	AWS Règle de configuration	Conseils
1490	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.
1490	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1501	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
1504	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
1504	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
1504	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1504	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1504	root-account-mfa-enabled	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authent ification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisa teur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
1509	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatc h pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
1509	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
1509	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
1509	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activat ion de plusieurs paramètre s. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrai l l'activation dans plusieurs régions.
1509	elasticsearch-logs-to-cloud watch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1509	api-gw-execution-logging-en abled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
1509	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
1509	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
1509	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1509	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
1509	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
1509	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
1509	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
1509	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.
1509	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.
1509	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	AWS Règle de configuration	Conseils
1509	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1511	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
1511	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
1511	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	AWS Règle de configuration	Conseils
1511	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1511	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1511	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
1511	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1511	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
1511	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.

ID du contrôle	AWS Règle de configuration	Conseils
1511	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1511	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1511	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1511	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1511	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.
1511	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
1511	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1511	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.
1515	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
1515	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
1515	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1515	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1515	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
1515	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.
1515	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
1515	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
1515	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1515	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1515	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.
1515	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
1515	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.
1536	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
1537	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
1537	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1552	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
1552	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
1552	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
1552	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
1552	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
1579	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
1580	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
1580	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
1580	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
1650	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
1650	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
1650	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
1650	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
1650	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1650	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
1650	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
1650	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
1650	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1650	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
1650	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
1650	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
1650	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
1650	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.
1650	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.
1650	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	AWS Règle de configuration	Conseils
1650	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1657	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1657	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
1657	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1657	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.
1657	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.
1657	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.

ID du contrôle	AWS Règle de configuration	Conseils
1657	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
1661	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
1661	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
1661	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
1661	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
1661	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1661	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
1661	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
1661	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
1661	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1661	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
1661	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
1661	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
1661	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
1661	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
1679	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
1679	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
1679	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1679	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1679	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
1680	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
1680	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
1680	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1680	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1680	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
1681	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
1681	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
1681	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1681	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1681	root-account-mfa-enabled	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authent ification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisa teur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
1683	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	AWS Règle de configuration	Conseils
1683	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
1690	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
1690	ec2-instance-managed-by-sys tems-manager	Un inventaire des plateform es logicielles et des applicati ons au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploit ation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1690	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateform e AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.
1690	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
1690	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.
1690	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1690	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1691	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
1691	ec2-instance-managed-by-systems-manager	Un inventaire des plateform es logicielles et des applicati ons au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploit ation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1691	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateform e AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.
1691	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
1691	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.
1691	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1691	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1693	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
1693	ec2-instance-managed-by-sys tems-manager	Un inventaire des plateform es logicielles et des applicati ons au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploit ation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1693	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateform e AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.
1693	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
1693	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.
1693	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1693	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1694	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
1695	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
1707	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.
P1	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
P1	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
P3	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	AWS Règle de configuration	Conseils
P5	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
P7	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
P7	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
P7	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
P7	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	AWS Règle de configuration	Conseils
P8	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
P9	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
P9	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
P9	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
P9	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	AWS Règle de configuration	Conseils
P9	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
P9	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
P9	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
P9	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
P9	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
P9	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
P9	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
P9	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
P9	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
P9	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
P10	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
P10	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
P10	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisate ur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommand e d'utiliser des politiques gérées plutôt que des politique s intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedAc tionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decry pt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
P10	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
P11	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for ACSC ISM.

Bonnes pratiques de fonctionnement pour l'IA et le ML

Ce pack de conformité contient des AWS Config règles basées sur l'IA et le ML. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for AI and ML.

Bonnes pratiques de fonctionnement pour Amazon API Gateway

Ce pack de conformité contient des AWS Config règles basées sur l'utilisation d'Amazon API Gateway au sein AWS de celui-ci. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for Amazon API Gateway.

Bonnes pratiques opérationnelles pour Amazon CloudWatch

Ce pack de conformité contient des AWS Config règles basées sur l'utilisation d'Amazon CloudWatch au sein AWS de celui-ci. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for Amazon CloudWatch.

Bonnes pratiques opérationnelles pour Amazon DynamoDB

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour Amazon DynamoDB.

Bonnes pratiques opérationnelles pour Amazon S3

Le modèle est disponible sur GitHub : Operational Best Practices for Amazon S3.

Bonnes pratiques de fonctionnement pour APRA CPG 234

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité

spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre l'Australian Prudential Regulation Authority (APRA) CPG 234 et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles APRA CPG 234. Un contrôle APRA CPG 234 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages vers les contrôles APRA CPG 234 2019, qui a été créé par le Commonwealth d'Australie et peut être consulté dans le Guide pratique prudentiel : sécurité des informations CPG 234. La licence du cadre en vertu de la Licence Creative Commons Australia Attribution 3.0 et les informations sur les droits d'auteur du cadre (y compris une exclusion de garanties) sont disponibles sur APRA | Droit d'auteur.

ID du contrôle	AWS Règle de configuration	Conseils
36a	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
36a	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour

ID du contrôle	AWS Règle de configuration	Conseils
		vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
36a	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politique s et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
36b	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
36b	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
36b	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
36b	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activat ion de plusieurs paramètre s. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrai l l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
36b	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36b	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
36b	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
36c	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisate urs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
36c	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
36c	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36c	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
36c	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
36c	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
36c	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
36c	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
36d	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
36d	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
36d	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36d	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
36d	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36d	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
36d	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
36d	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
36d	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
36d	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
36d	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36d	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
36d	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
36d	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
36d	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
36d	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36d	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
36d	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
36d	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
36d	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
36d	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
36d	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
36d	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
36d	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36d	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
36d	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
36d	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
36d	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
36d	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
36d	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
36d	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisate ur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommand e d'utiliser des politiques gérées plutôt que des politique s intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedAc tionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decry pt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.
36d	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'associa tion d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
36d	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
36d	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
36d	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
36d	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
36d	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	AWS Règle de configuration	Conseils
36d	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
36d	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
36d	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
36d	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
36d	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
36e	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	AWS Règle de configuration	Conseils
36e	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctem ent transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
36e	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
36e	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36e	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
36e	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
36e	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36e	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
36e	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
36e	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
36e	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
36e	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
36e	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36e	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
36e	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
36e	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
36e	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
36e	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
36e	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
36e	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
36e	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	AWS Règle de configuration	Conseils
36e	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
36e	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
36e	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	AWS Règle de configuration	Conseils
36e	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
36e	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
36e	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
36f	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36f	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
36f	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36f	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
36f	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36f	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
36f	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
36f	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
36f	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
36f	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
36f	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
36f	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
36f	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
36f	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
36f	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
36f	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
36f	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36f	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
36f	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
36f	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.
36f	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
36f	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
36f	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	AWS Règle de configuration	Conseils
36f	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
36f	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
36f	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	AWS Règle de configuration	Conseils
36f	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
36f	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
36f	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
36g	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
36g	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
36g	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36h	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
36h	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
36h	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36h	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
36h	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
36h	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
36h	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36h	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
36i	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	AWS Règle de configuration	Conseils
36i	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
36i	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
36i	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
36i	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.
36i	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	AWS Règle de configuration	Conseils
36i	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
36i	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
36i	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
36i	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modificat ions de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'applica tion. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifié s et d'identifier les causes possibles à étudier.
36i	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
36j	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
36j	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
36j	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.
36j	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
36j	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	AWS Règle de configuration	Conseils
36j	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
36j	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThreshodPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.
36j	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	AWS Règle de configuration	Conseils
36j	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
36j	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modificat ions de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'applica tion. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifié s et d'identifier les causes possibles à étudier.
36j	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
36l	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
36l	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
36l	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.
36l	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
36l	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
36l	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
36l	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
36l	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponi ble. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indispo nibilité de votre passerelle client, vous pouvez configure r une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
36l	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
36l	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
36l	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
36l	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.
36l	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
36l	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
36l	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
36l	beanstalk-enhanced-health-r eporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modificat ions de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'applica tion. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifié s et d'identifier les causes possibles à étudier.

ID du contrôle	AWS Règle de configuration	Conseils
39(a)(b)(d)	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
39(a)(b)(d)	guardduty-non-archived-find ings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classific ations pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSev (Config Default : 30), daysMediu mSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisat ion.

ID du contrôle	AWS Règle de configuration	Conseils
39(a)(b)(d)	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
40	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politique s et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
40	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
40	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
40	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
44a	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
44a	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
44a	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
44b	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
44b	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
44b	elb-deletion-protection-ena bled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applicati ons.

ID du contrôle	AWS Règle de configuration	Conseils
44c	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
44c	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
44c	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
44c	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
45	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
45	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
45	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
45	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
45	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
45	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
45	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
45	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
45	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
45	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
45	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
45	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
45	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
45	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
45	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
45	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
45	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
45	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
45	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
45	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
45	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
45	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
45	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
45	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
45	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
45	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
45	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
45	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
45	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
45	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
45	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
45	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisate ur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommand e d'utiliser des politiques gérées plutôt que des politique s intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedAc tionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decry pt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.
45	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'associa tion d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
45	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
45	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
45	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
45	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
45	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
45	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.
45	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
45	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
45	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
47c	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
47c	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
47c	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
47c	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
47c	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
47c	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
52c	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
52c	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
52c	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
52c	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
52c	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
52c	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
52c	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
52c	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
52c	s3-bucket-server-side-encry ption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartim ents Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
52c	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
52c	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
52c	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
52c	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
52c	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
52c	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
52c	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
52c	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
52c	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
52d	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
52d	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
52d	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
52d	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
52d	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
52d	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
52d	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
52d	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
52d	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
52d	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
52d	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
52d	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
52d	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
52d	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
52d	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
52d	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
52d	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
52d	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
52d	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionn alités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.
52d	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involonta ire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
52d	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
52d	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communica tion sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
52d	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
52e	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
52e	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
53	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
53	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
53	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
53	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
53	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
53	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
53	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
53	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
53	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
53	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
53	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
53	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
53	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
53	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
53	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
53	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
53	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
53	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
53	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
53	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
53	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionn alités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
53	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
53	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
54	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
54	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
54	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
54	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
54	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
54	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
54	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
54	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
54	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
54	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
54	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
54	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
54	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
54	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
54	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
54	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
54	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
54	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
54	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
54	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
54	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
54	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
54	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
54	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
54	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
54	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
55	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
55	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
67	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
67	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
67	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
67	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
67	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
67	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
67	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
67	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
67	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
67	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
67	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
67	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
67	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
67	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
67	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
67	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
67	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
67	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
68	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
68	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
73	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
73	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
AttachmentA_1(b)(h)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(b)(h)	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
AttachmentA_1(b)(h)	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'associa tion d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(c)	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
AttachmentA_1(c)	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
AttachmentA_1(e)	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
AttachmentA_1(e)	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
AttachmentA_1(e)	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
AttachmentA_1(e)	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
AttachmentA_1(e)	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
AttachmentA_1(e)	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentA_1(e)	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
AttachmentA_1(e)	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentB_1	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibili sation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
AttachmentC_4	access-keys-rotated	Les informations d'identif ication sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organis ation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
AttachmentC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
AttachmentC_4	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
AttachmentC_4	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
AttachmentC_4	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AttachmentC_4	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisate ur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommand e d'utiliser des politiques gérées plutôt que des politique s intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedAc tionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decry pt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.
AttachmentC_4	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'associa tion d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_4	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
AttachmentC_5	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_5	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
AttachmentC_5	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_5	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_5	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
AttachmentC_6	root-account-hardware-mfa-e nabled	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_6	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
AttachmentC_6	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(c)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
AttachmentC_7(h)	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AttachmentC_7(h)	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
AttachmentC_7(h)	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
AttachmentC_7(h)	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
AttachmentC_7(h)	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
AttachmentC_7(h)	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(h)	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
AttachmentC_7(h)	elasticsearch-logs-to-cloud watch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(i)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(j)	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisate urs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
AttachmentC_7(j)	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisate urs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protectio n, en plus des informations d'identification de connexion . En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_7(j)	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
AttachmentC_7(j)	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_8	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
AttachmentC_8	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AttachmentC_8	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_8	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
AttachmentC_8	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_8	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_8	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_8	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
AttachmentC_8	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_8	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
AttachmentC_8	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentC_8	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
AttachmentD_1	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentD_1	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
AttachmentE_4	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
AttachmentE_4	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_5(d)	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
AttachmentE_1(a)(b)(d)	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
AttachmentE_1(a)(b)(d)	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
AttachmentE_1(a)(b)(d)	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AttachmentE_1(a)(b)(d)	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
AttachmentE_1(a)(b)(d)	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
AttachmentE_1(a)(b)(d)	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
AttachmentE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AttachmentE_1(a)(b)(d)	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
AttachmentE_1(a)(b)(d)	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
AttachmentE_1(a)(b)(d)	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AttachmentE_1(a)(b)(d)	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
AttachmentE_1(a)(b)(d)	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
AttachmentE_1(a)(b)(d)	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
AttachmentE_1(a)(b)(d)	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
AttachmentE_1(a)(b)(d)	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
AttachmentE_1(a)(b)(d)	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
AttachmentE_1(a)(b)(d)	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
AttachmentE_1(a)(b)(d)	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour l'APRA CPG 234.

Bonnes pratiques de fonctionnement pour la gestion des ressources

Ce pack de conformité contient des AWS Config règles basées sur la gestion des actifs qu'il contient. AWS Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour la gestion des actifs.

Bonnes pratiques de fonctionnement pour AWS Backup

Ce pack de conformité contient des AWS Config règles basées sur l' AWS Backup intérieur AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for AWS Backup.

Bonnes pratiques opérationnelles pour la gestion des AWS identités et des accès

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour la gestion des AWS identités et des accès.

Meilleures pratiques opérationnelles pour le pilier de fiabilité du AWS framework Well-Architected

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le pilier de fiabilité Well-Architected Framework d'Amazon Web Services et AWS les règles de configuration gérées. Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs principes de conception du pilier. Une catégorie de cadre Well-Architected peut être associée à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-1	Comment gérer les quotas et les contraintes de service ? Pour les architectures de charge de travail basées sur le Cloud, il existe des quotas de service (également appelés limites de service). Ces	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	quotas permettent d'éviter de fournir accidentellement plus de ressources que nécessaire et de limiter les taux de demande des opérations d'API afin de protéger les services de tout abus. Il existe également des contraintes de ressources, par exemple la vitesse à laquelle les bits peuvent être transmis par un câble à fibre optique ou la quantité de données stockées sur un disque physique.		charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-1	Comment gérer les quotas et les contraintes de service ? Pour les architectures de charge de travail basées sur le Cloud, il existe des quotas de service (également appelés limites de service). Ces quotas permettent d'éviter de fournir accidentellement plus de ressources que nécessaire et de limiter les taux de demande des opérations d'API afin de protéger les services de tout abus. Il existe également des contraintes de ressources, par exemple la vitesse à laquelle les bits peuvent être transmis par un câble à fibre optique ou la quantité de données stockées sur un disque physique.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-1	Comment gérer les quotas et les contraintes de service ? Pour les architectures de charge de travail basées sur le Cloud, il existe des quotas de service (également appelés limites de service). Ces quotas permettent d'éviter de fournir accidentellement plus de ressources que nécessaire et de limiter les taux de demande des opérations d'API afin de protéger les services de tout abus. Il existe également des contraintes de ressources, par exemple la vitesse à laquelle les bits peuvent être transmis par un câble à fibre optique ou la quantité de données stockées sur un disque physique.	ecs-task-definition-memory-hard-limit	Limiter la mémoire maximale disponible sur vos conteneurs Amazon Elastic Container Service (ECS) garantit que vos ressources ne peuvent pas être utilisées de manière abusive en cas d'accès malveillant à vos conteneurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-2	Comment planifier la topologie de votre réseau ? Les charges de travail existent souvent dans plusieurs environnements. Il s'agit notamment de plusieurs environnements Cloud (accessibles au public et privés) et éventuellement de votre infrastructure de centre de données existante. Les plans doivent inclure des considérations relatives au réseau, telles que la connectivité intra- et inter-systèmes, la gestion des adresses IP publiques, la gestion des adresses IP privées et la résolution des noms de domaine.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-2	Comment planifier la topologie de votre réseau ? Les charges de travail existent souvent dans plusieurs environnements. Il s'agit notamment de plusieurs environnements Cloud (accessibles au public et privés) et éventuellement de votre infrastructure de centre de données existante. Les plans doivent inclure des considérations relatives au réseau, telles que la connectivité intra- et inter-systèmes, la gestion des adresses IP publiques, la gestion des adresses IP privées et la résolution des noms de domaine.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-2	Comment planifier la topologie de votre réseau ? Les charges de travail existent souvent dans plusieurs environnements. Il s'agit notamment de plusieurs environnements Cloud (accessibles au public et privés) et éventuellement de votre infrastructure de centre de données existante. Les plans doivent inclure des considérations relatives au réseau, telles que la connectivité intra- et inter-systèmes, la gestion des adresses IP publiques, la gestion des adresses IP privées et la résolution des noms de domaine.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-5	Comment concevoir les interactions dans un système distribué afin d'atténuer les défaillances ou d'y résister ? Les systèmes distribué s s'appuient sur des réseaux de communication pour interconnecter les composants, comme les serveurs ou les services. Votre charge de travail doit fonctionner de manière fiable malgré la perte de données ou la latence sur ces réseaux. Les composants du système distribué doivent fonctionn er de manière à ne pas avoir d'impact négatif sur les autres composants ou sur la charge de travail. Ces bonnes pratiques permettent d'éviter les défaillances et d'améliorer le temps	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	moyen entre défaillances (MTBF).		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	ecs-container-insights-enabled	La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Elastic Container Service (ECS) et de vos AWS solutions. Conteneur Insights fournit également des informations de diagnostic (par exemple sur les échecs de redémarrage des conteneurs) pour vous aider à isoler les problèmes et à les résoudre rapidement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement Multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-6	Comment surveiller les ressources de charge de travail ? Les journaux et les métriques sont des outils puissants qui permettent de mieux comprendre l'état de santé de votre charge de travail. Vous pouvez configurer votre charge de travail pour qu'elle surveille les journaux et les métriques et envoie des notifications lorsque des seuils sont franchis ou que des événements importants se produisent. La surveillance permet à votre charge de travail de reconnaître le franchissement de seuils de faible performance ou l'apparition de défaillances, afin qu'elle puisse se rétablir automatiquement en réponse.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-7	Comment concevoir votre charge de travail pour qu'elle s'adapte à l'évolution de la demande ? Une charge de travail évolutive permet d'ajouter ou de supprimer automatiquement des ressources de manière à ce qu'elles correspondent à la demande actuelle à un moment donné.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-7	Comment concevoir votre charge de travail pour qu'elle s'adapte à l'évoluti on de la demande ? Une charge de travail évolutive permet d'ajouter ou de supprimer automatiq uement des ressource s de manière à ce qu'elles correspon dent à la demande actuelle à un moment donné.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-7	Comment concevoir votre charge de travail pour qu'elle s'adapte à l'évolution de la demande ? Une charge de travail évolutive permet d'ajouter ou de supprimer automatiquement des ressources de manière à ce qu'elles correspondent à la demande actuelle à un moment donné.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-8	Comment mettre en œuvre des modifications ? Des modifications maîtrisées sont nécessaires afin de déployer de nouvelles fonctionnalités et de garantir que les charges de travail et l'environnement d'exploitation utilisent des logiciels connus et qu'ils peuvent être corrigés ou remplacés de manière prévisible. Si ces modifications ne sont pas maîtrisées, il devient difficile d'en prévoir les effets ou de résoudre les problèmes qui en découlent.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-8	Comment mettre en œuvre des modifications ? Des modifications maîtrisées sont nécessaires afin de déployer de nouvelles fonctionnalités et de garantir que les charges de travail et l'environnement d'exploitation utilisent des logiciels connus et qu'ils peuvent être corrigés ou remplacés de manière prévisible. Si ces modifications ne sont pas maîtrisées, il devient difficile d'en prévoir les effets ou de résoudre les problèmes qui en découlent.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-8	Comment mettre en œuvre des modifications ? Des modifications maîtrisées sont nécessaires afin de déployer de nouvelles fonctionnalités et de garantir que les charges de travail et l'environnement d'exploitation utilisent des logiciels connus et qu'ils peuvent être corrigés ou remplacés de manière prévisible. Si ces modifications ne sont pas maîtrisées, il devient difficile d'en prévoir les effets ou de résoudre les problèmes qui en découlent.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-8	Comment mettre en œuvre des modifications ? Des modifications maîtrisées sont nécessaires afin de déployer de nouvelles fonctionnalités et de garantir que les charges de travail et l'environnement d'exploitation utilisent des logiciels connus et qu'ils peuvent être corrigés ou remplacés de manière prévisible. Si ces modifications ne sont pas maîtrisées, il devient difficile d'en prévoir les effets ou de résoudre les problèmes qui en découlent.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-9	Comment sauvegarder les données ? Sauvegardez les données, les applications et la configuration pour répondre à vos exigences en matière d'objectifs de délai de reprise (RTO) et de points de reprise (RPO).	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-10	Comment utiliser l'isolation des pannes pour protéger votre charge de travail ? Les périmètres d'isolation des pannes limitent l'effet d'une panne au sein d'une charge de travail à un nombre limité de composants. Les composants situés en dehors du périmètre ne sont pas affectés par la défaillance. En utilisant plusieurs périmètres d'isolati on des pannes, vous pouvez limiter l'impact sur votre charge de travail.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-10	Comment utiliser l'isolation des pannes pour protéger votre charge de travail ? Les périmètres d'isolation des pannes limitent l'effet d'une panne au sein d'une charge de travail à un nombre limité de composants. Les composants situés en dehors du périmètre ne sont pas affectés par la défaillance. En utilisant plusieurs périmètres d'isolati on des pannes, vous pouvez limiter l'impact sur votre charge de travail.	clb-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibi lité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-10	Comment utiliser l'isolation des pannes pour protéger votre charge de travail ? Les périmètres d'isolation des pannes limitent l'effet d'une panne au sein d'une charge de travail à un nombre limité de composants. Les composants situés en dehors du périmètre ne sont pas affectés par la défaillance. En utilisant plusieurs périmètres d'isolati on des pannes, vous pouvez limiter l'impact sur votre charge de travail.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibi lité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-10	Comment utiliser l'isolation des pannes pour protéger votre charge de travail ? Les périmètres d'isolation des pannes limitent l'effet d'une panne au sein d'une charge de travail à un nombre limité de composants. Les composants situés en dehors du périmètre ne sont pas affectés par la défaillance. En utilisant plusieurs périmètres d'isolati on des pannes, vous pouvez limiter l'impact sur votre charge de travail.	lambda-vpc-multi-az-check	Si votre fonction AWS Lambda est configuré e pour se connecter à un cloud privé virtuel (VPC) dans votre compte, déployez la fonction AWS Lambda dans au moins deux zones de disponibi lité différentes afin de vous assurer que votre fonction est disponible pour traiter les événements en cas d'interruption de service dans une seule zone.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-10	Comment utiliser l'isolation des pannes pour protéger votre charge de travail ? Les périmètres d'isolation des pannes limitent l'effet d'une panne au sein d'une charge de travail à un nombre limité de composants. Les composants situés en dehors du périmètre ne sont pas affectés par la défaillance. En utilisant plusieurs périmètres d'isolati on des pannes, vous pouvez limiter l'impact sur votre charge de travail.	opensearch-data-no de-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) nécessite au moins trois nœuds de données pour garantir une haute disponibilité et une tolérance aux pannes. Le déploieme nt d'un domaine de OpenSearch service comportant au moins trois nœuds de données garantit les opérations du cluster en cas de défaillance d'un nœud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-10	Comment utiliser l'isolation des pannes pour protéger votre charge de travail ? Les périmètres d'isolation des pannes limitent l'effet d'une panne au sein d'une charge de travail à un nombre limité de composants. Les composants situés en dehors du périmètre ne sont pas affectés par la défaillance. En utilisant plusieurs périmètres d'isolati on des pannes, vous pouvez limiter l'impact sur votre charge de travail.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
REL-10	Comment utiliser l'isolation des pannes pour protéger votre charge de travail ? Les périmètres d'isolation des pannes limitent l'effet d'une panne au sein d'une charge de travail à un nombre limité de composants. Les composants situés en dehors du périmètre ne sont pas affectés par la défaillance. En utilisant plusieurs périmètres d'isolati on des pannes, vous pouvez limiter l'impact sur votre charge de travail.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for AWS Well-Architected Reliability Pillar.

Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le pilier de sécurité Well-Architected Framework d'Amazon Web Services et AWS les règles de configuration gérées. Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs principes de conception du pilier. Une catégorie de cadre Well-Architected peut être associée à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les processus que vous avez définis dans le cadre de l'excellence opération nelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommand ations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous permet de mettre à l'échelle vos opération s de sécurité.		des configura tions de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opération nelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommand ations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opération nelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommand ations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opération nelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommand ations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opérationnelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommandations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opérationnelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommandations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opérationnelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommandations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opération nelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommand ations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opérationnelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommandations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-1	Comment gérer votre charge de travail en toute sécurité ? Pour gérer votre charge de travail en toute sécurité, vous devez appliquer les bonnes pratiques générales à tous les domaines de sécurité. Prenez les exigences et les processus que vous avez définis dans le cadre de l'excellence opérationnelle au niveau de l'organisation et de la charge de travail, et appliquez-les à tous les domaines. Le fait de rester à jour avec AWS les recommandations du secteur et les informations sur les menaces vous permet de faire évoluer votre modèle de menace et vos objectifs de contrôle. L'automatisation des processus de sécurité, des tests et de la validation vous	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild . AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permet de mettre à l'échelle vos opération s de sécurité.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	secretsmanager-secret-periodic-rotation	Cette règle garantit que AWS la rotation périodique des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis. La valeur par défaut est 90 jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-2	Comment gérer les identités des personnes et des machines ? Il existe deux types d'identités que vous devez gérer lorsque vous abordez des AWS charges de travail sécurisées. Comprendre le type d'identité dont vous avez besoin pour gérer et accorder les accès vous permet de vous assurer que les bonnes identités ont accès aux bonnes ressources dans les bonnes conditions. Identités humaines : vos administrateurs, développeurs, opérateurs et utilisateurs finaux ont besoin d'une identité pour accéder à vos AWS environnements et à vos applications. Il s'agit de membres de votre organisation ou d'utilisateurs externes avec lesquels vous collaborez et qui	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	interagissent avec vos AWS ressources via un navigateur Web, une application cliente ou des outils de ligne de commande interactifs. Identités des machines : vos applications de service, vos outils opérationnels et vos charges de travail ont besoin d'une identité pour envoyer des demandes aux AWS services, par exemple pour lire des données. Ces identités incluent les machines exécutées dans votre AWS environnement, telles que les instances Amazon EC2 ou les fonctions Lambda AWS . Vous pouvez également gérer les Identités machine pour les parties externes qui ont besoin d'un accès. En outre, il se peut AWS que des machines extérieures aient		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	besoin d'accéder à votre AWS environnement.		
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairemen t qui ou quoi doit avoir accès à chaque composant, choisisse z le type d'identit é approprié et la méthode d'authent ification et d'autoris ation.	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairemen t qui ou quoi doit avoir accès à chaque composant, choisisse z le type d'identit é approprié et la méthode d'authent ification et d'autoris ation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Chaque composant ou ressource de votre charge de travail doit être accessible aux administrateurs, aux utilisateurs finaux ou à d'autres composants. Définissez clairement qui ou quoi doit avoir accès à chaque composant, choisissez le type d'identité approprié et la méthode d'authentification et d'autorisation.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Établissez des contrôles communs qui limitent l'accès à toutes les identités de votre organisation. Par exemple, vous pouvez restreindre l'accès à des AWS régions spécifiques ou empêcher vos opérateurs de supprimer des ressources communes, telles qu'un rôle IAM utilisé par votre équipe de sécurité centrale	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveille z en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressource s nécessitant ce type d'accès.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveille z en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressource s nécessitant ce type d'accès.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveille z en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressource s nécessitant ce type d'accès.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveille z en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressource s nécessitant ce type d'accès.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveille z en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressource s nécessitant ce type d'accès.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveille z en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressource s nécessitant ce type d'accès.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-3	Comment gérer les autorisations des personnes et des machines ? Surveillez en permanence les résultats qui mettent en évidence l'accès public et l'accès intercompte. Réduisez l'accès public et l'accès intercompte aux seules ressources nécessitant ce type d'accès.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événements de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événements de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	cw-loggroup-retent ion-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisant e pour faciliter le dépannage et les enquêtes judiciair es. Le manque de données disponibl es dans les journaux d'événements passés complique la reconstit ution et l'identification des événement s potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événements de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événements de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événements de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événements de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-4	Comment détecter les événements de sécurité et comment y répondre ? Capturez et analysez les événements à partir des journaux et des métriques pour gagner en visibilité. Prenez des mesures en cas d'événeme nts de sécurité et de menaces potentielles afin de sécuriser votre charge de travail.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	ec2-instance-multiple-eni-check	Cette règle vérifie si vos instances Amazon Elastic Compute Cloud (Amazon EC2) ont plusieurs ENI. Le fait d'avoir plusieurs ENI peut entraîner la création d'instances à double connexion, c'est-à-dire d'instances ayant plusieurs sous-réseaux. Cela peut ajouter à la complexité de la sécurité du réseau et introduire des chemins et des accès non intentionnels au réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Interne t ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources informatiques ? Les ressources informati ques de votre charge de travail nécessite nt plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneur s, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans condition s peut entraîner un comportement involontaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-5	Comment protéger vos ressources réseau ? Toute charge de travail disposant d'une certaine forme de connectivité réseau, qu'il s'agisse d'Internet ou d'un réseau privé, nécessite plusieurs couches de défense pour se protéger des menaces externes et internes basées sur le réseau.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informati ques de votre charge de travail nécessite nt plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneur s, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ecs-container-insights-enabled	La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Elastic Container Service (ECS) et de vos AWS solutions. Conteneur Insights fournit également des informations de diagnostic (par exemple sur les échecs de redémarrage des conteneurs) pour vous aider à isoler les problèmes et à les résoudre rapidement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informati ques de votre charge de travail nécessite nt plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneur s, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiq uement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-for me. Pour faciliter la gestion des correctif s de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-instance-multiple-eni-check	Cette règle vérifie si vos instances Amazon Elastic Compute Cloud (Amazon EC2) ont plusieurs ENI. Le fait d'avoir plusieurs ENI peut entraîner la création d'instances à double connexion, c'est-à-dire d'instances ayant plusieurs sous-réseaux. Cela peut ajouter à la complexité de la sécurité du réseau et introduire des chemins et des accès non intentionnels au réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-6	Comment protéger vos ressources informatiques ? Les ressources informatiques de votre charge de travail nécessitent plusieurs couches de protection contre les menaces externes et internes. Les ressources de calcul incluent les instances EC2, les conteneurs, les fonctions AWS Lambda, les services de base de données, les appareils IoT, etc.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles, afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-v ous que le chiffreme nt est activé pour vos Amazon CloudWatch Log Groups.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	dynamodb-table-enc rypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffreme nt au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principal e propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SEC-8	Comment protéger vos données au repos ? Protégez vos données au repos en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de mauvaise gestion.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SEC-9	Comment protéger vos données en transit ? Protégez vos données en transit en mettant en place plusieurs contrôles , afin de réduire le risque d'accès non autorisé ou de perte.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for AWS Well-Architected Security Pillar.

Bonnes pratiques de fonctionnement pour le BCP et la DR

Ce pack de conformité contient des AWS Config règles basées sur le BCP et le DR. AWS Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for BCP and DR.

Bonnes pratiques de fonctionnement pour BNM RMiT

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les règles de gestion des risques technologiques (RMiT) de Bank Negara Malaysia (BNM) et les règles de configuration gérées AWS . Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles BNM RMiT. Un contrôle BNM RMiT peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures approprié es pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financièr es ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatibl e avec leur propensio n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,18	Une institution financière doit faire preuve de diligence raisonnable et évaluer les contrôles cryptographiques associés à la technologie utilisée afin de protéger la confidentialité, l'intégrité, l'authentification, l'autorisation et la non-répudiation des informations. Lorsqu'une institution financière ne génère pas ses propres clés de chiffrement, elle doit prendre les mesures appropriées pour garantir la mise en place de contrôles et de processus robustes pour gérer les clés de chiffrement. Si les institutions financières ont recours à des évaluations tierces, elles doivent déterminer si ce recours est compatible avec leur propensio	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n et leur tolérance au risque. Une instituti on financière doit également tenir dûment compte des ressources système requises pour la prise en charge des contrôles cryptogra phiques et du risque de réduction de la visibilité du trafic réseau des données chiffrées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,20	Une institution financière doit stocker les clés cryptographiques publiques dans un certificat délivré par une autorité de certification, en fonction du niveau de risque. Ces certificats associés aux clients doivent être délivrés par des autorités de certification reconnues. L'institution financière doit veiller à ce que la mise en œuvre de protocoles d'authentification et de signature utilisant de tels certificats fasse l'objet d'une protection solide afin de garantir que l'utilisation de clés cryptographiques privées correspondant aux certificats utilisateur soit juridiquement contraignante et irréfutable. L'émission initiale et le renouvellement ultérieur de	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tels certificats doivent être conformes aux bonnes pratiques du secteur et aux spécifications légales/réglementaires applicables.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,20	Une institution financière doit stocker les clés cryptographiques publiques dans un certificat délivré par une autorité de certification, en fonction du niveau de risque. Ces certificats associés aux clients doivent être délivrés par des autorités de certification reconnues. L'institution financière doit veiller à ce que la mise en œuvre de protocoles d'authentification et de signature utilisant de tels certificats fasse l'objet d'une protection solide afin de garantir que l'utilisation de clés cryptographiques privées correspondant aux certificats utilisateur soit juridiquement contraignante et irréfutable. L'émission initiale et le renouvellement ultérieur de	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tels certificats doivent être conformes aux bonnes pratiques du secteur et aux spécifications légales/ réglementaires applicables.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	beanstalk-enhanced -health-reporting- enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrast ructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibi lité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournisse nt un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,27	Une institution financière doit établir des mécanisme s de surveillance en temps réel pour suivre l'utilisation des capacités et les performances des processus, ainsi que des services clés. Ces mécanismes de surveillance doivent être capables de fournir des alertes rapides et exploitables aux administrateurs.	rds-enhanced-monit oring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibi lité d'Amazon RDS. Vous disposez ainsi d'une visibilit é détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploieme nt multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,34	Une institution financière doit veiller à ce que les services réseau de ses systèmes critiques soient fiables et exempts de SPOF afin de protéger les systèmes critiques contre les défaillances potentielles du réseau et les cybermenaces.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,34	Une institution financière doit veiller à ce que les services réseau de ses systèmes critiques soient fiables et exempts de SPOF afin de protéger les systèmes critiques contre les défaillances potentielles du réseau et les cybermenaces.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,35	Une institution financière doit établir des processus de surveillance de la bande passante du réseau en temps réel et des métriques de résilience du service réseau correspon dantes pour signaler toute utilisation excessive de la bande passante et toute interruption du système résultant d'une surcharge de la bande passante ou de défaillances du réseau. Ces processus incluent l'analyse du trafic en vue de détecter les tendances et les anomalies.	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualise r, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimis ation. Assurez-v ous que X-Ray est activé afin que vous puissiez consulter des informations détaillée s non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microserv ices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,35	Une institution financière doit établir des processus de surveillance de la bande passante du réseau en temps réel et des métriques de résilience du service réseau correspon dantes pour signaler toute utilisation excessive de la bande passante et toute interruption du système résultant d'une surcharge de la bande passante ou de défaillances du réseau. Ces processus incluent l'analyse du trafic en vue de détecter les tendances et les anomalies.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,35	Une institution financière doit établir des processus de surveillance de la bande passante du réseau en temps réel et des métriques de résilience du service réseau correspondantes pour signaler toute utilisation excessive de la bande passante et toute interruption du système résultant d'une surcharge de la bande passante ou de défaillances du réseau. Ces processus incluent l'analyse du trafic en vue de détecter les tendances et les anomalies.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,35	Une institution financière doit établir des processus de surveillance de la bande passante du réseau en temps réel et des métriques de résilience du service réseau correspondantes pour signaler toute utilisation excessive de la bande passante et toute interruption du système résultant d'une surcharge de la bande passante ou de défaillances du réseau. Ces processus incluent l'analyse du trafic en vue de détecter les tendances et les anomalies.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,36	Une institution financière doit veiller à ce que les services réseau prenant en charge les systèmes critiques sont conçus et mis en œuvre de manière à garantir la confidentialité, l'intégrité et la disponibilité des données.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
10,36	Une institution financière doit veiller à ce que les services réseau prenant en charge les systèmes critiques sont conçus et mis en œuvre de manière à garantir la confidentialité, l'intégrité et la disponibilité des données.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,36	Une institution financière doit veiller à ce que les services réseau prenant en charge les systèmes critiques sont conçus et mis en œuvre de manière à garantir la confidentialité, l'intégrité et la disponibilité des données.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
10,36	Une institution financière doit veiller à ce que les services réseau prenant en charge les systèmes critiques sont conçus et mis en œuvre de manière à garantir la confidentialité, l'intégrité et la disponibilité des données.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,36	Une institution financière doit veiller à ce que les services réseau prenant en charge les systèmes critiques sont conçus et mis en œuvre de manière à garantir la confidentialité, l'intégrité et la disponibilité des données.	nlb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos Network Load Balancers (NLB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,38	Une institution financière doit veiller à ce que des journaux de périphériques réseau suffisants et pertinents soient conservés pendant au moins trois ans à des fins d'enquêtes et d'analyse scientifique.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection approprié es concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'el le utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés . Ces mesures de protection comprenne nt le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriéta ires et des services hébergés sur le cloud, notamment la gestion des clés cryptogra phiques pertinentes.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès, en veillant à ce que les utilisateurs IAM soient membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs IAM. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs IAM.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,51	Une institution financière doit mettre en œuvre des mesures de protection appropriées concernant les informations des clients et des contreparties, ainsi que les données propriétaires lorsqu'elle utilise des services cloud afin de se protéger contre toute divulgation et tout accès non autorisés. Ces mesures de protection comprennent le maintien de la propriété, du contrôle et de la gestion de toutes les données relatives aux clients, des informations des contreparties, des données propriétaires et des services hébergés sur le cloud, notamment la gestion des clés cryptographiques pertinentes.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisat eurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	account-part-of-or ganizations	La gestion centralis ée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernan ce centralisée des comptes peut entraîner des configura tions de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisat eurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisat eurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisat eurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès, en veillant à ce que les utilisateurs IAM soient membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisat eurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs IAM. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs IAM.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisat eurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,52	Une institution financière doit mettre en œuvre une politique de contrôle d'accès appropriée pour l'identification, l'authentification et l'autorisation des utilisateurs (utilisateurs internes et externes tels que les fournisseurs de services tiers). Cette politique doit couvrir les contrôles d'accès à la technologie à la fois logiques et physiques, lesquels sont proportionnels au niveau de risque d'accès non autorisé aux systèmes technologiques de cette institution	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(b)(h)(i)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins lorsque seules les autorisations minimales suffisantes sont accordées aux utilisateurs légitimes pour assumer leurs rôles ; (h) limiter et contrôler le partage des identifiants d'utilisateur et des mots de passe entre plusieurs utilisateurs ; et (i) contrôler l'utilisation de conventions génériques de dénomination des identifiants d'utilisateur en faveur d'identifiants plus personnellement identifiables.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(b)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins, en accordant uniquement les autorisations minimales suffisantes aux utilisateurs légitimes pour qu'ils assument leurs rôles ;	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(b)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins, en accordant uniquemen t les autorisations minimales suffisant es aux utilisateurs légitimes pour qu'ils assument leurs rôles ;	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(b)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins, en accordant uniquement les autorisations minimales suffisantes aux utilisateurs légitimes pour qu'ils assument leurs rôles ;	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
10.53(b)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins, en accordant uniquement les autorisations minimales suffisantes aux utilisateurs légitimes pour qu'ils assument leurs rôles ;	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(b)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins, en accordant uniquement les autorisations minimales suffisantes aux utilisateurs légitimes pour qu'ils assument leurs rôles ;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(b)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins, en accordant uniquement les autorisations minimales suffisantes aux utilisateurs légitimes pour qu'ils assument leurs rôles ;	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès, en veillant à ce que les utilisateurs IAM soient membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(b)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (b) utiliser les droits d'accès « de moindre privilège » ou basés sur les besoins, en accordant uniquement les autorisations minimales suffisantes aux utilisateurs légitimes pour qu'ils assument leurs rôles ;	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(c)(f)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (c) utiliser des droits d'accès limités dans le temps qui restreignent l'accès à une période spécifique, y compris les droits d'accès accordés aux fournisseurs de services ; (f) appliquer une authentification plus stricte pour les activités critiques, notamment l'accès à distance	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(f)(h)	Conformément au paragraphe 10.52, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (f) adopter une authentification plus stricte pour les activités critiques , notamment pour l'accès à distance ; (h) limiter et contrôler le partage des identifia nts d'utilisateur et des mots de passe entre plusieurs utilisateurs	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs IAM. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs IAM.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(f)(h)	Conformément au paragraphe 10.54, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (f) adopter une authentification plus stricte pour les activités critiques , notamment pour l'accès à distance ; (h) limiter et contrôler le partage des identifiants d'utilisateur et des mots de passe entre plusieurs utilisateurs	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.53(f)(h)	Conformément au paragraphe 10.54, une institution financière doit intégrer les principes suivants à sa politique de contrôle d'accès : (f) adopter une authentification plus stricte pour les activités critiques , notamment pour l'accès à distance ; (h) limiter et contrôler le partage des identifiants d'utilisateur et des mots de passe entre plusieurs utilisateurs	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,54	Une institution financière doit utiliser des processus d'authentification robustes pour garantir l'authenticité des identités utilisées . Les mécanisme s d'authentification doivent être proportio nnels à la criticité des fonctions et adopter au moins un de ces trois facteurs d'authentification de base, à savoir ce que l'utilisateur connaît (par exemple un mot de passe, un code PIN), un élément qu'il possède (par exemple une carte à puce, un dispositi f de sécurité) et ce qu'il est (par exemple, des caractéristiques biométriques, telles qu'une empreinte digitale ou un motif rétinien).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs IAM. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs IAM.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,54	Une institution financière doit utiliser des processus d'authentification robustes pour garantir l'authenticité des identités utilisées . Les mécanisme s d'authentification doivent être proportio nnels à la criticité des fonctions et adopter au moins un de ces trois facteurs d'authentification de base, à savoir ce que l'utilisateur connaît (par exemple un mot de passe, un code PIN), un élément qu'il possède (par exemple une carte à puce, un dispositi f de sécurité) et ce qu'il est (par exemple, des caractéristiques biométriques, telles qu'une empreinte digitale ou un motif rétinien).	root-account-hardw are-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,54	Une institution financière doit utiliser des processus d'authentification robustes pour garantir l'authenticité des identités utilisées . Les mécanisme s d'authentification doivent être proportio nnels à la criticité des fonctions et adopter au moins un de ces trois facteurs d'authentification de base, à savoir ce que l'utilisateur connaît (par exemple un mot de passe, un code PIN), un élément qu'il possède (par exemple une carte à puce, un dispositi f de sécurité) et ce qu'il est (par exemple, des caractéristiques biométriques, telles qu'une empreinte digitale ou un motif rétinien).	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,55	Une institution financière doit revoir et adapter régulièrement ses pratiques en matière de mots de passe afin de renforcer sa résilience face à l'évolution des attaques. Ces pratiques comprennent la génération efficace et sécurisée des mots de passe. Des contrôles appropriés doivent être mis en place pour vérifier le niveau de sécurité des mots de passe créés.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,56	Les méthodes d'authentification qui dépendent de plusieurs facteurs sont généralem ent plus difficiles à compromettre qu'un système utilisant un seul facteur. Dans cette optique, les institutions financières sont encouragées à concevoir et à mettre en œuvre (en particuli er dans les systèmes à haut risque ou utilisant l'« authentif ication unique ») une authentification multifactorielle (MFA) plus fiable et plus dissuasive contre la fraude	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs IAM. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs IAM.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,56	Les méthodes d'authentification qui dépendent de plusieurs facteurs sont généralement plus difficiles à compromettre qu'un système utilisant un seul facteur. Dans cette optique, les institutions financières sont encouragées à concevoir et à mettre en œuvre (en particulier dans les systèmes à haut risque ou utilisant l'« authentification unique ») une authentification multifactorielle (MFA) plus fiable et plus dissuasive contre la fraude	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,56	Les méthodes d'authentification qui dépendent de plusieurs facteurs sont généralem ent plus difficiles à compromettre qu'un système utilisant un seul facteur. Dans cette optique, les institutions financières sont encouragées à concevoir et à mettre en œuvre (en particuli er dans les systèmes à haut risque ou utilisant l'« authentif ication unique ») une authentification multifactorielle (MFA) plus fiable et plus dissuasive contre la fraude	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisate urs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourci r la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	account-part-of-or ganizations	La gestion centralis ée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernan ce centralisée des comptes peut entraîner des configura tions de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès, en veillant à ce que les utilisateurs IAM soient membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillé s efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activit é doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,59	Une institution financière doit veiller à ce que (a) les contrôles d'accès aux systèmes à l'échelle de l'entreprise soient gérés et surveillés efficacement ; et (b) les activités des utilisateurs dans les systèmes critiques soient journalisées à des fins d'audit et d'enquêtes. Les journaux d'activité doivent être conservés pendant au moins trois ans et révisés régulièrement en temps opportun.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,60	Pour satisfaire à l'exigence du paragraphe 10.59, les grandes instituti ons financières sont tenues de (a) déployer un système de gestion des accès aux identités afin de gérer et de surveiller efficacement l'accès des utilisateurs aux systèmes de l'entreprise ; et (b) déployer des outils d'audit automatisés pour signaler toute anomalie.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,60	Pour satisfaire à l'exigence du paragraphe 10.61, les grandes instituti ons financières sont tenues de (a) déployer un système de gestion des accès aux identités afin de gérer et de surveiller efficacement l'accès des utilisateurs aux systèmes de l'entreprise ; et (b) déployer des outils d'audit automatisés pour signaler toute anomalie.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,60	Pour satisfaire à l'exigence du paragraphe 10.61, les grandes instituti ons financières sont tenues de (a) déployer un système de gestion des accès aux identités afin de gérer et de surveiller efficacement l'accès des utilisateurs aux systèmes de l'entreprise ; et (b) déployer des outils d'audit automatisés pour signaler toute anomalie.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,61	Une institution financière doit s'assurer que les systèmes critiques ne fonctionnent pas sur des systèmes obsolètes présentant des vulnérabilités de sécurité connues ou des systèmes technologiques end-of-life (EOL). À cet égard, une institution financière doit clairement attribuer des responsabilités aux fonctions définies : (a) pour surveiller en permanence et mettre en œuvre les dernières versions de correctifs en temps opportun ; et (b) pour identifier les systèmes technologiques critiques qui approchent de leur fin de vie afin d'appliquer des mesures correctives supplémentaires.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,61	Une institution financière doit s'assurer que les systèmes critiques ne fonctionnent pas sur des systèmes obsolètes présentant des vulnérabilités de sécurité connues ou des systèmes technologiques end-of-life (EOL). À cet égard, une institution financière doit clairement attribuer des responsabilités aux fonctions définies : (a) pour surveiller en permanence et mettre en œuvre les dernières versions de correctifs en temps opportun ; et (b) pour identifier les systèmes technologiques critiques qui approchent de leur fin de vie afin d'appliquer des mesures correctives supplémentaires.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,61	Une institution financière doit s'assurer que les systèmes critiques ne fonctionnent pas sur des systèmes obsolètes présentant des vulnérabilités de sécurité connues ou des systèmes technologiques end-of-life (EOL). À cet égard, une institution financière doit clairement attribuer des responsabilités aux fonctions définies : (a) pour surveiller en permanence et mettre en œuvre les dernières versions de correctifs en temps opportun ; et (b) pour identifier les systèmes technologiques critiques qui approchent de leur fin de vie afin d'appliquer des mesures correctives supplémentaires.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,61	Une institution financière doit s'assurer que les systèmes critiques ne fonctionnent pas sur des systèmes obsolètes présentant des vulnérabilités de sécurité connues ou des systèmes technologiques end-of-life (EOL). À cet égard, une institution financière doit clairement attribuer des responsabilités aux fonctions définies : (a) pour surveiller en permanence et mettre en œuvre les dernières versions de correctifs en temps opportun ; et (b) pour identifier les systèmes technologiques critiques qui approchent de leur fin de vie afin d'appliquer des mesures correctives supplémentaires.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10,61	Une institution financière doit s'assurer que les systèmes critiques ne fonctionnent pas sur des systèmes obsolètes présentant des vulnérabilités de sécurité connues ou des systèmes technologiques end-of-life (EOL). À cet égard, une institution financière doit clairement attribuer des responsabilités aux fonctions définies : (a) pour surveiller en permanence et mettre en œuvre les dernières versions de correctifs en temps opportun ; et (b) pour identifier les systèmes technologiques critiques qui approchent de leur fin de vie afin d'appliquer des mesures correctives supplémentaires.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	api-gw-cache-enabl ed-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environne ment API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	backup-recovery-po int-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	opensearch-encrypt ed-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	sagemaker-endpoint -configuration-kms- key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	sagemaker-notebook -instance-kms-key- configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-note s, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confidentialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(a)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (a) la confident ialité et l'intégrité des informations, ainsi que des transactions des clients et des contreparties	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(b)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (b) la fiabilité des services fournis par le biais de canaux et d'appareils garantissant une interruption minimale des services	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(b)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (b) la fiabilité des services fournis par le biais de canaux et d'appareils garantiss ant une interruption minimale des services	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.
10.64(b)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (b) la fiabilité des services fournis par le biais de canaux et d'appareils garantiss ant une interruption minimale des services	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(b)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (b) la fiabilité des services fournis par le biais de canaux et d'appareils garantiss ant une interruption minimale des services	nlb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos NetworkLo ad équilibreurs (NLB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(b)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (b) la fiabilité des services fournis par le biais de canaux et d'appareils garantissant une interruption minimale des services	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(b)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (b) la fiabilité des services fournis par le biais de canaux et d'appareils garantiss ant une interruption minimale des services	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(b)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (b) la fiabilité des services fournis par le biais de canaux et d'appareils garantissant une interruption minimale des services	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(d)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (d) une piste d'audit suffisante et une surveillance des transactions anormales	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technolog iques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.64(e)	Une institution financière doit mettre en œuvre des contrôles de sécurité technologiques robustes pour fournir des services numériques qui garantissent ce qui suit : (e) la capacité d'identifier et de revenir au point de récupération avant un incident ou une interruption de service	s3-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos compartiments Amazon Simple Storage Service (S3) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.7	Une institution financière doit déployer des outils efficaces pour prendre en charge la surveillance continue et proactive, ainsi que la détection rapide des activités anormales dans son infrastructure technologique. La portée de la surveillance doit couvrir tous les systèmes critiques, y compris l'infrastructure annexe.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.7	Une institution financière doit déployer des outils efficaces pour prendre en charge la surveillance continue et proactive, ainsi que la détection rapide des activités anormales dans son infrastructure technologique. La portée de la surveillance doit couvrir tous les systèmes critiques, y compris l'infrastructure annexe.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.8	Une institution financière doit veiller à ce que ses opération s de cybersécu rité préviennent et détectent en permanence toute violation potentiel le de ses contrôles de sécurité ou tout affaiblissement de sa posture de sécurité. Les grandes instituti ons financières doivent notamment réaliser une évaluatio n trimestrielle des vulnérabilités des composants réseau externes et internes qui prennent en charge tous les systèmes critiques.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.8	Une institution financière doit veiller à ce que ses opération s de cybersécu rité préviennent et détectent en permanence toute violation potentiel le de ses contrôles de sécurité ou tout affaiblissement de sa posture de sécurité. Les grandes instituti ons financières doivent notamment réaliser une évaluatio n trimestrielle des vulnérabilités des composants réseau externes et internes qui prennent en charge tous les systèmes critiques.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.18(c)(f)	Le SOC doit être en mesure d'assumer les fonctions suivantes : (c) la gestion des vulnérabilités ; (f) fournir une meilleure visibilité de la situation pour détecter les adversaires et les menaces, y compris l'analyse et les opérations de renseignement sur les menaces, ainsi que la surveillance des indicateurs de compromission (IOC). Cette démarche inclut une analyse comportementale avancée pour détecter les logiciels malveillants sans signature et sans fichier et pour identifier les anomalies susceptibles de constituer des menaces de sécurité, notamment au niveau des points de terminaison et des couches réseau.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.18(c)(f)	Le SOC doit être en mesure d'assumer les fonctions suivantes : (c) la gestion des vulnérabilités ; (f) fournir une meilleure visibilité de la situation pour détecter les adversaires et les menaces, y compris l'analyse et les opérations de renseignement sur les menaces, ainsi que la surveillance des indicateurs de compromission (IOC). Cette démarche inclut une analyse comportementale avancée pour détecter les logiciels malveillants sans signature et sans fichier et pour identifier les anomalies susceptibles de constituer des menaces de sécurité, notamment au niveau des points de terminaison et des couches réseau.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.18(c)(f)	Le SOC doit être en mesure d'assumer les fonctions suivantes : (c) la gestion des vulnérabilités ; (f) fournir une meilleure visibilité de la situation pour détecter les adversaires et les menaces, y compris l'analyse et les opérations de renseignement sur les menaces, ainsi que la surveillance des indicateurs de compromission (IOC). Cette démarche inclut une analyse comportementale avancée pour détecter les logiciels malveillants sans signature et sans fichier et pour identifier les anomalies susceptibles de constituer des menaces de sécurité, notamment au niveau des points de terminaison et des couches réseau.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.1	Révisez régulièrement les paramètres de configuration et de règles de tous les dispositifs de sécurité. Utilisez des outils automatisés pour examiner et surveiller les modifications apportées aux paramètres de configuration et de règles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.1	Révisez régulièrement les paramètres de configuration et de règles de tous les dispositifs de sécurité. Utilisez des outils automatisés pour examiner et surveiller les modifications apportées aux paramètres de configuration et de règles.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.5(b)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (b) utilisation de tunnels sécurisés tels que le protocole TLS (Transport Layer Security) et le réseau privé virtuel (VPN) IPsec	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe 5.5(b)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (b) utilisation de tunnels sécurisés tels que le protocole TLS (Transport Layer Security) et le réseau privé virtuel (VPN) IPsec	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.5(b)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (b) utilisation de tunnels sécurisés tels que le protocole TLS (Transport Layer Security) et le réseau privé virtuel (VPN) IPsec	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.5(b)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (b) utilisation de tunnels sécurisés tels que le protocole TLS (Transport Layer Security) et le réseau privé virtuel (VPN) IPsec	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.5(b)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (b) utilisation de tunnels sécurisés tels que le protocole TLS (Transport Layer Security) et le réseau privé virtuel (VPN) IPsec	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe 5.5(b)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (b) utilisation de tunnels sécurisés tels que le protocole TLS (Transport Layer Security) et le réseau privé virtuel (VPN) IPsec	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.5(c)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (c) déploiement de serveurs intermédiaires dotés de défenses périmétriques et de protections adéquates, telles qu'un pare-feu, un IPS et un antivirus.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.5(c)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (c) déploiement de serveurs intermédiaires dotés de défenses périmétriques et de protections adéquates, telles qu'un pare-feu, un IPS et un antivirus.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.5(c)	Assurez-vous que les contrôles de sécurité pour les connexions réseau server-to-server externes incluent les éléments suivants : (c) déploiement de serveurs intermédiaires dotés de défenses périmétriques et de protections adéquates, telles qu'un pare-feu, un IPS et un antivirus.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.6	Assurez-vous que les contrôles de sécurité de l'accès à distance au serveur incluent les éléments suivants : (a) la limitation de l'accès aux seuls dispositifs de points de terminaison sécurisés et verrouillés ; (b) l'utilisation de tunnels sécurisés tels que TLS et VPN IPsec ; (c) le déploiement d'un serveur « passerelle » doté de défenses périmétriques et d'une protection adéquates, telles qu'un pare-feu, un IPS et un antivirus ; et (d) la fermeture des ports concernés immédiatement après l'expiration de l'accès à distance.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.6	Assurez-vous que les contrôles de sécurité de l'accès à distance au serveur incluent les éléments suivants : (a) la limitation de l'accès aux seuls dispositifs de points de terminaison sécurisés et verrouillés ; (b) l'utilisation de tunnels sécurisés tels que TLS et VPN IPsec ; (c) le déploiement d'un serveur « passerelle » doté de défenses périmétriques et d'une protection adéquates, telles qu'un pare-feu, un IPS et un antivirus ; et (d) la fermeture des ports concernés immédiatement après l'expiration de l'accès à distance.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.6	Assurez-vous que les contrôles de sécurité de l'accès à distance au serveur incluent les éléments suivants : (a) la limitation de l'accès aux seuls dispositifs de points de terminaison sécurisés et verrouillés ; (b) l'utilisation de tunnels sécurisés tels que TLS et VPN IPsec ; (c) le déploiement d'un serveur « passerelle » doté de défenses périmétriques et d'une protection adéquates, telles qu'un pare-feu, un IPS et un antivirus ; et (d) la fermeture des ports concernés immédiatement après l'expiration de l'accès à distance.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.6	Assurez-vous que les contrôles de sécurité de l'accès à distance au serveur incluent les éléments suivants : (a) la limitation de l'accès aux seuls dispositifs de points de terminaison sécurisés et verrouillés ; (b) l'utilisation de tunnels sécurisés tels que TLS et VPN IPsec ; (c) le déploiement d'un serveur « passerelle » doté de défenses périmétriques et d'une protection adéquates, telles qu'un pare-feu, un IPS et un antivirus ; et (d) la fermeture des ports concernés immédiatement après l'expiration de l'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.6	Assurez-vous que les contrôles de sécurité de l'accès à distance au serveur incluent les éléments suivants : (a) la limitation de l'accès aux seuls dispositifs de points de terminaison sécurisés et verrouillés ; (b) l'utilisation de tunnels sécurisés tels que TLS et VPN IPsec ; (c) le déploiement d'un serveur « passerelle » doté de défenses périmétriques et d'une protection adéquates, telles qu'un pare-feu, un IPS et un antivirus ; et (d) la fermeture des ports concernés immédiatement après l'expiration de l'accès à distance.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 5.6	Assurez-vous que les contrôles de sécurité de l'accès à distance au serveur incluent les éléments suivants : (a) la limitation de l'accès aux seuls dispositifs de points de terminaison sécurisés et verrouillés ; (b) l'utilisation de tunnels sécurisés tels que TLS et VPN IPsec ; (c) le déploiement d'un serveur « passerelle » doté de défenses périmétriques et d'une protection adéquates, telles qu'un pare-feu, un IPS et un antivirus ; et (d) la fermeture des ports concernés immédiatement après l'expiration de l'accès à distance.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (a)	Une institution financière doit concevoir une architecture cloud robuste et veiller à ce que cette conceptio n soit conforme aux normes internati onales pertinentes pour l'application prévue.	account-part-of-or ganizations	La gestion centralis ée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernan ce centralisée des comptes peut entraîner des configura tions de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (b)	Les institutions financières sont encouragées à adopter des principes de confiance zéro afin de fournir une architecture cyberrésiliente en adoptant une approche fondée sur l'hypothèse d'une violation, en combinant la microsegmentation, le « refus defense-in-depth par défaut », les droits d'accès fondés sur le « moindre privilège », et en procédant à une inspection approfondie et à une validation continue, le cas échéant.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (b)	Les institutions financières sont encouragées à adopter des principes de confiance zéro afin de fournir une architecture cyberrésiliente en adoptant une approche fondée sur l'hypothèse d'une violation, en combinant la microsegmentation, le « refus defense-in-depth par défaut », les droits d'accès fondés sur le « moindre privilège », et en procédant à une inspection approfondie et à une validation continue, le cas échéant.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (b)	Les institutions financières sont encouragées à adopter des principes de confiance zéro afin de fournir une architecture cyberrésiliente en adoptant une approche fondée sur l'hypothèse d'une violation, en combinant la microsegmentation, le « refus defense-in-depth par défaut », les droits d'accès fondés sur le « moindre privilège », et en procédant à une inspection approfondie et à une validation continue, le cas échéant.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (b)	Les institutions financières sont encouragées à adopter des principes de confiance zéro afin de fournir une architecture cyberrésiliente en adoptant une approche fondée sur l'hypothèse d'une violation, en combinant la microsegmentation, le « refus defense-in-depth par défaut », les droits d'accès fondés sur le « moindre privilège », et en procédant à une inspection approfondie et à une validation continue, le cas échéant.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (c)	Une institution financière doit utiliser l'approche d'architecture réseau la plus récente ainsi que des concepts et solutions de conception de réseau appropriés pour gérer et surveiller la sécurité granulaire du réseau et la fourniture centralisée du réseau afin de gérer la complexité de l'environnement réseau dans le cloud.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (c)	Une institution financière doit utiliser l'approche d'architecture réseau la plus récente ainsi que des concepts et solutions de conception de réseau appropriés pour gérer et surveiller la sécurité granulaire du réseau et la fourniture centralisée du réseau afin de gérer la complexité de l'environnement réseau dans le cloud.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
Annexe 10 Partie B - 1 (d)	Une institution financière doit établir et utiliser des canaux de communication sécurisés et chiffrés pour migrer les serveurs physiques, les applications ou les données vers les plateformes cloud.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (d)	Une institution financière doit établir et utiliser des canaux de communication sécurisés et chiffrés pour migrer les serveurs physiques , les applications ou les données vers les plateformes cloud.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (f) i)	L'utilisation croissante d'interfaces de programmation d'applications (API) par les institutions financières pour s'interconnecter avec des fournisseurs de services d'applications externes est susceptible d'améliorer l'efficacité de la prestation de nouveaux services. Cette tendance peut toutefois augmenter la surface des cyberattaques et une mauvaise gestion peut amplifier l'impact d'un incident de sécurité de l'information. Une institution financière doit veiller à ce que ses API soient soumises à des mécanismes de gestion et de contrôle rigoureux, en garantissant notamment les points suivants : i) les API doivent être	api-gwv2-authorization-type-configured	Assurez-vous que votre routage d'API Amazon API Gateway v2 présente un type d'autorisation défini pour empêcher tout accès non autorisé aux ressources backend sous-jacentes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	conçues pour garantir la résilience des services afin d'éviter le risque de points de défaillance uniques et elles doivent être configurées de manière sécurisée avec des contrôles d'accès appropriés ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (f) (ii)	L'utilisation croissante d'interfaces de programmation d'applications (API) par les institutions financières pour s'interconnecter avec des fournisseurs de services d'applications externes est susceptible d'améliorer l'efficacité de la prestation de nouveaux services. Cette tendance peut toutefois augmenter la surface des cyberattaques et une mauvaise gestion peut amplifier l'impact d'un incident de sécurité de l'information. Une institution financière doit veiller à ce que ses API soient soumises à des mécanismes de gestion et de contrôle rigoureux, en garantissant notamment les points suivants : ii) les API doivent être suivies et	[api-gw-associated-with-waf](#)	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	surveillées par rapport aux cyberattaques avec des mesures de réponse aux incidents adéquates et être mises hors service rapidement lorsqu'el les ne sont plus utilisées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 1 (f) (ii)	L'utilisation croissante d'interfaces de programmation d'applications (API) par les institutions financières pour s'interconnecter avec des fournisseurs de services d'applications externes est susceptible d'améliorer l'efficacité de la prestation de nouveaux services. Cette tendance peut toutefois augmenter la surface des cyberattaques et une mauvaise gestion peut amplifier l'impact d'un incident de sécurité de l'information. Une institution financière doit veiller à ce que ses API soient soumises à des mécanismes de gestion et de contrôle rigoureux, en garantissant notamment les points suivants : ii) les API doivent être suivies et	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	surveillées par rapport aux cyberattaques avec des mesures de réponse aux incidents adéquates et être mises hors service rapidement lorsqu'el les ne sont plus utilisées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 2 (b) ii)	Une institution financière doit continuellement tirer parti des capacités améliorées du cloud pour renforcer la sécurité des services cloud et les instituti ons financières sont, entre autres, encouragées à : ii) utiliser des pratiques d'infrastructure immuables pour le déploiement des services afin de réduire le risque de défaillance en créant un nouvel environnement doté de la dernière version stable du logiciel. La surveillance continue de l'environ nement cloud doit inclure l'automat isation de la détection des modifications apportées à l'infrast ructure immuable afin d'améliorer le contrôle de la conformité et la lutte contre les	cloudformation-stack-notification-check	Pour détecter les modifications involontaires apportées aux AWS ressources sous-jacentes, assurez-vous que votre CloudFormation stack est configuré pour envoyer des notificat ions d'événements à une rubrique Amazon SNS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	cyberattaques en constante évolution		
Annexe 10 Partie B - 3 (b) vi)	Une institution financière doit veiller à ce que les images des machines virtuelles et des conteneurs soient configurées, renforcées et surveillées de manière appropriée. Cette démarche inclut les éléments suivants : vi) les images stockées sont soumises à une surveillance de sécurité contre tout accès et toute modification non autorisés.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (a) i)	Afin de garantir une fonctionnalité de reprise efficace, les institutions financièr es doivent veiller à ce que les procédure s de sauvegarde et de restauration existantes soient étendues aux services cloud, notamment en procédant comme suit : i) définir et formalise r une stratégie de sauvegarde et de restauration au stade de la planification de l'adoption du cloud ;	aurora-resources-p rotected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (a) i)	Afin de garantir une fonctionnalité de reprise efficace, les institutions financièr es doivent veiller à ce que les procédure s de sauvegarde et de restauration existantes soient étendues aux services cloud, notamment en procédant comme suit : i) définir et formalise r une stratégie de sauvegarde et de restauration au stade de la planification de l'adoption du cloud ;	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (a) i)	Afin de garantir une fonctionnalité de reprise efficace, les institutions financières doivent veiller à ce que les procédures de sauvegarde et de restauration existantes soient étendues aux services cloud, notamment en procédant comme suit : i) définir et formaliser une stratégie de sauvegarde et de restauration au stade de la planification de l'adoption du cloud ;	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (a) i)	Afin de garantir une fonctionnalité de reprise efficace, les institutions financières doivent veiller à ce que les procédures de sauvegarde et de restauration existantes soient étendues aux services cloud, notamment en procédant comme suit : i) définir et formaliser une stratégie de sauvegarde et de restauration au stade de la planification de l'adoption du cloud ;	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (a) i)	Afin de garantir une fonctionnalité de reprise efficace, les institutions financières doivent veiller à ce que les procédures de sauvegarde et de restauration existantes soient étendues aux services cloud, notamment en procédant comme suit : i) définir et formaliser une stratégie de sauvegarde et de restauration au stade de la planification de l'adoption du cloud ;	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (a) i)	Afin de garantir une fonctionnalité de reprise efficace, les institutions financières doivent veiller à ce que les procédures de sauvegarde et de restauration existantes soient étendues aux services cloud, notamment en procédant comme suit : i) définir et formaliser une stratégie de sauvegarde et de restauration au stade de la planification de l'adoption du cloud ;	s3-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos compartiments Amazon Simple Storage Service (S3) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (b)	Une institution financière doit veiller à ce que les procédures de sauvegarde et de restauration soient testées périodiquement afin de valider les fonctionnalités de reprise. La fréquence des procédures de sauvegarde doit être proportionnelle à la criticité du système et à l'objectif de point de reprise (RPO) du système. Des mesures correctives doivent être prises rapidement par l'institution financière en cas d'échec des sauvegardes.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (c) i)	Un établissement financier doit garantir une sauvegarde et une restauration suffisantes de la machine virtuelle et du conteneur, y compris les paramètres de configuration de sauvegarde (pour l'IaaS et le PaaS, le cas échéant), notamment les éléments suivants : i) garantir la capacité de restaurer une machine virtuelle et un conteneur point-in-time conformément aux objectifs de reprise d'activité ;	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (d) i)	Une institution financière doit évaluer les exigences de résilience des services cloud et identifier les mesures appropriées adaptées à la criticité du système, afin de garantir la disponibi lité des services dans les scénarios les plus défavorables. Les institutions financières doivent envisager une approche fondée sur le risque et adopter progressivement des contrôles d'atténua tion appropriés pour garantir la disponibi lité des services et atténuer le risque de concentration. Parmi les options viables figurent : i) tirer parti des fonctionnalités de haute disponibi lité et de redondanc e des services cloud pour garantir que les centres de données de productio	autoscaling-multiple-az	Pour garantir une haute disponibilité, assurez-vous que votre groupe Auto Scaling est configuré pour couvrir plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n disposent d'une capacité redondant e dans les différent es zones de disponibi lité ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (d) i)	Une institution financière doit évaluer les exigences de résilience des services cloud et identifier les mesures appropriées adaptées à la criticité du système, afin de garantir la disponibilité des services dans les scénarios les plus défavorables. Les institutions financières doivent envisager une approche fondée sur le risque et adopter progressivement des contrôles d'atténuation appropriés pour garantir la disponibilité des services et atténuer le risque de concentration. Parmi les options viables figurent : i) tirer parti des fonctionnalités de haute disponibilité et de redondance des services cloud pour garantir que les centres de données de productio	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiquement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n disposent d'une capacité redondant e dans les différent es zones de disponibi lité ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (d) i)	Une institution financière doit évaluer les exigences de résilience des services cloud et identifier les mesures appropriées adaptées à la criticité du système, afin de garantir la disponibilité des services dans les scénarios les plus défavorables. Les institutions financières doivent envisager une approche fondée sur le risque et adopter progressivement des contrôles d'atténuation appropriés pour garantir la disponibilité des services et atténuer le risque de concentration. Parmi les options viables figurent : i) tirer parti des fonctionnalités de haute disponibilité et de redondance des services cloud pour garantir que les centres de données de productio	lambda-vpc-multi-az-check	Si votre fonction AWS Lambda est configurée pour se connecter à un cloud privé virtuel (VPC) dans votre compte, déployez la fonction AWS Lambda dans au moins deux zones de disponibilité différentes afin de vous assurer que votre fonction est disponible pour traiter les événements en cas d'interruption de service dans une seule zone.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n disposent d'une capacité redondant e dans les différent es zones de disponibi lité ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (d) i)	Une institution financière doit évaluer les exigences de résilience des services cloud et identifier les mesures appropriées adaptées à la criticité du système, afin de garantir la disponibilité des services dans les scénarios les plus défavorables. Les institutions financières doivent envisager une approche fondée sur le risque et adopter progressivement des contrôles d'atténuation appropriés pour garantir la disponibilité des services et atténuer le risque de concentration. Parmi les options viables figurent : i) tirer parti des fonctionnalités de haute disponibilité et de redondance des services cloud pour garantir que les centres de données de productio	nlb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos NetworkLoad équilibreurs (NLB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n disposent d'une capacité redondant e dans les différent es zones de disponibi lité ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (d) i)	Une institution financière doit évaluer les exigences de résilience des services cloud et identifier les mesures appropriées adaptées à la criticité du système, afin de garantir la disponibilité des services dans les scénarios les plus défavorables. Les institutions financières doivent envisager une approche fondée sur le risque et adopter progressivement des contrôles d'atténuation appropriés pour garantir la disponibilité des services et atténuer le risque de concentration. Parmi les options viables figurent : i) tirer parti des fonctionnalités de haute disponibilité et de redondance des services cloud pour garantir que les centres de données de productio	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n disposent d'une capacité redondant e dans les différent es zones de disponibi lité ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 5 (d) i)	Une institution financière doit évaluer les exigences de résilience des services cloud et identifier les mesures appropriées adaptées à la criticité du système, afin de garantir la disponibilité des services dans les scénarios les plus défavorables. Les institutions financières doivent envisager une approche fondée sur le risque et adopter progressivement des contrôles d'atténuation appropriés pour garantir la disponibilité des services et atténuer le risque de concentration. Parmi les options viables figurent : i) tirer parti des fonctionnalités de haute disponibilité et de redondance des services cloud pour garantir que les centres de données de productio	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	n disposent d'une capacité redondant e dans les différent es zones de disponibi lité ;		cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement approprié es et pertinentes pour protéger la confident ialité et l'intégrité des données sensibles stockées dans le cloud.	api-gw-cache-enabl ed-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environne ment API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	eks-secrets-encrypted	Pour protéger les données au repos, assurez-vous que la configuration de vos clusters Amazon Elastic Kubernetes Service (Amazon EKS) soit compatible avec le chiffrement des secrets Kubernetes. Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (a)	Une institution financière doit mettre en œuvre des techniques de chiffrement appropriées et pertinentes pour protéger la confidentialité et l'intégrité des données sensibles stockées dans le cloud.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (d)	Avec l'adoption croissante du cloud, la gestion de nombreuses clés de chiffrement utilisées pour protéger les données est devenue plus complexe et peut introduire de nouveaux défis pour les institutions financières. Une institution financière doit adopter une approche globale et centralisée en matière de gestion des clés, notamment en utilisant un système de gestion des clés centralisé capable de gérer les générations, le stockage et la distribution des clés de manière sécurisée et évolutive.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 8 (d)	Avec l'adoption croissante du cloud, la gestion de nombreuses clés de chiffrement utilisées pour protéger les données est devenue plus complexe et peut introduire de nouveaux défis pour les institutions financières. Une institution financière doit adopter une approche globale et centralisée en matière de gestion des clés, notamment en utilisant un système de gestion des clés centralisé capable de gérer les générations, le stockage et la distribution des clés de manière sécurisée et évolutive.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 9 (a) ii)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières devraient veiller à l'utilisation de contrôles stricts pour accéder au plan de gestion, qui peuvent inclure les éléments suivants : ii) mettre en œuvre le « moindre privilège » et une authentification multifactorielle forte (MFA), par exemple un mot de passe fort, un jeton logiciel, un outil de gestion	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des accès privilégiés et des fonctions de vérification ;		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 9 (a) ii)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières devraient veiller à l'utilisation de contrôles stricts pour accéder au plan de gestion, qui peuvent inclure les éléments suivants : ii) mettre en œuvre le « moindre privilège » et une authentification multifactorielle forte (MFA), par exemple un mot de passe fort, un jeton logiciel, un outil de gestion	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs IAM. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs IAM.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des accès privilégiés et des fonctions de vérification ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 9 (a) ii)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières devraient veiller à l'utilisation de contrôles stricts pour accéder au plan de gestion, qui peuvent inclure les éléments suivants : ii) mettre en œuvre le « moindre privilège » et une authentification multifactorielle forte (MFA), par exemple un mot de passe fort, un jeton logiciel, un outil de gestion	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des accès privilégiés et des fonctions de vérification ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 9 (a) ii)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières devraient veiller à l'utilisation de contrôles stricts pour accéder au plan de gestion, qui peuvent inclure les éléments suivants : ii) mettre en œuvre le « moindre privilège » et une authentification multifactorielle forte (MFA), par exemple un mot de passe fort, un jeton logiciel, un outil de gestion	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des accès privilégiés et des fonctions de vérification ;		
Annexe 10 Partie B - 9 (a) iii)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières doivent garantir l'utilisation de contrôles stricts pour accéder au plan de gestion, en procédant comme suit : iii) utiliser une attribution granulaire des droits des utilisateurs privilégiés ;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 9 (a) iii)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières doivent garantir l'utilisation de contrôles stricts pour accéder au plan de gestion, en procédant comme suit : iii) utiliser une attribution granulaire des droits des utilisateurs privilégiés ;	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 9 (a) iv)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières doivent veiller à utiliser des contrôles stricts pour accéder au plan de gestion, en procédant comme suit : iv) réaliser une surveillance continue des activités effectuées par les utilisateurs privilégiés ;	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 9 (a) iv)	Le plan de gestion constitue une différence de sécurité essentielle entre l'infrastructure traditionnelle et le cloud computing, où l'accès à distance est pris en charge par défaut. Cette couche d'accès peut être sujette aux cyberattaques, compromettant ainsi l'intégrité du déploiement dans le cloud. Dans cette optique, les institutions financières doivent veiller à utiliser des contrôles stricts pour accéder au plan de gestion, en procédant comme suit : iv) réaliser une surveillance continue des activités effectuées par les utilisateurs privilégiés ;	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 12 (a)	Une institution financière doit protéger les données hébergées dans les services cloud conformément à la section Prévention contre la perte de données (paragrap hes 11.14 à 11.16) de la présente politique, notamment en augmentant l'empreinte des points de terminaison si l'institution financière autorise ses collabora teurs à utiliser leurs propres appareils pour accéder aux données sensibles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 12 (a)	Une institution financière doit protéger les données hébergées dans les services cloud conformément à la section Prévention contre la perte de données (paragraphes 11.14 à 11.16) de la présente politique, notamment en augmentant l'empreinte des points de terminaison si l'institution financière autorise ses collaborateurs à utiliser leurs propres appareils pour accéder aux données sensibles.	macie-status-check	Amazon Macie est un service dédié à la sécurité des données qui utilise le machine learning (ML) et la correspondance de modèles pour identifier et protéger vos données sensibles dans les compartiments Amazon Simple Storage Service (Amazon S3).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 14 (c) i)	Une institution financière doit envisager les mesures supplémen taires suivantes dans le cadre de l'élaboration de son CIRP : i) améliorer sa capacité à détecter les incidents de sécurité afin de garantir une gestion efficace des incidents , y compris la capacité à détecter les fuites de données sur le dark Web ;	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Annexe 10 Partie B - 14 (c) i)	Une institution financière doit envisager les mesures supplémentaires suivantes dans le cadre de l'élaboration de son CIRP : i) améliorer sa capacité à détecter les incidents de sécurité afin de garantir une gestion efficace des incidents, y compris la capacité à détecter les fuites de données sur le dark Web ;	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for BNM RMiT.

Bonnes pratiques de fonctionnement pour le profil moyen de contrôle du cloud du Canadian Centre for Cyber Security (CCCS)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le profil de contrôle du cloud moyen du Centre canadien pour la cybersécurité (CCCS) et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CCCS Medium Cloud Control Profile. Un contrôle de profil moyen de contrôle du cloud CCCS peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(1)	Gestion de compte AC-2(1) | Gestion automatisée des comptes système	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(3)	Gestion des comptes AC-2(3) | Désactiver les comptes inactifs	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(3)	Gestion des comptes AC-2(3) | Désactiver les comptes inactifs	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(4)	Gestion des comptes AC-2 (4) | Actions de vérification automatisées	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-AC-2(4)	Gestion des comptes AC-2 (4) | Actions de vérification automatisées	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(4)	Gestion des comptes AC-2 (4) | Actions de vérification automatisées	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(4)	Gestion des comptes AC-2 (4) | Actions de vérification automatisées	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2(4)	Gestion des comptes AC-2 (4) | Actions de vérification automatisées	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(4)	Gestion des comptes AC-2 (4) | Actions de vérification automatisées	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2(4)	Gestion des comptes AC-2 (4) | Actions de vérification automatisées	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.A	Gestion des comptes AC-2.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.B	Gestion des comptes AC-2.B	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.C	Gestion des comptes AC-2.C	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.D	Gestion des comptes AC-2.D	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.E	Gestion des comptes AC-2.E	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.F	Gestion des comptes AC-2.F	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.G	Gestion des comptes AC-2.G	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.H	Gestion des comptes AC-2.H	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.l	Gestion des comptes AC-2.l	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.l	Gestion des comptes AC-2.l	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.l	Gestion des comptes AC-2.l	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.l	Gestion des comptes AC-2.l	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.I	Gestion des comptes AC-2.I	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.J	Gestion des comptes AC-2.J	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-2.K	Gestion des comptes AC-2.K	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informati ons administratives sur chaque principal.
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-3.A	Exécution d'accès AC-3.A	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4(21)	Exécution des flux d'informations AC-4(21) | Séparation physique/logique des flux d'informations	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-4.A	Exécution du flux d'informations AC-4.A	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-5.A	Séparation des tâches AC-5.A	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-5.A	Séparation des tâches AC-5.A	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-5.A	Séparation des tâches AC-5.A	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-5.A	Séparation des tâches AC-5.A	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-5.A	Séparation des tâches AC-5.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(1)	Moindre privilège AC-6(1) | Autoriser l'accès aux fonctions de sécurité	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(1)	Moindre privilège AC-6(1) | Autoriser l'accès aux fonctions de sécurité	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(1)	Moindre privilège AC-6(1) | Autoriser l'accès aux fonctions de sécurité	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(1)	Moindre privilège AC-6(1) | Autoriser l'accès aux fonctions de sécurité	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(1)	Moindre privilège AC-6(1) | Autoriser l'accès aux fonctions de sécurité	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(2)	Moindre privilège AC-6(2) | Accès non privilégié pour les fonctions non liées à la sécurité	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(2)	Moindre privilège AC-6(2) | Accès non privilégié pour les fonctions non liées à la sécurité	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(2)	Moindre privilège AC-6(2) | Accès non privilégié pour les fonctions non liées à la sécurité	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(2)	Moindre privilège AC-6(2) | Accès non privilégié pour les fonctions non liées à la sécurité	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(2)	Moindre privilège AC-6(2) | Accès non privilégié pour les fonctions non liées à la sécurité	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(5)	Moindre privilège AC-6(5) | Comptes privilégiés	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(5)	Moindre privilège AC-6(5) | Comptes privilégiés	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(5)	Moindre privilège AC-6(5) | Comptes privilégiés	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(5)	Moindre privilège AC-6(5) | Comptes privilégiés	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(9)	Moindre privilège AC-6 (9) | Audit de l'utilisation des fonctions privilégiées	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-AC-6(9)	Moindre privilège AC-6 (9) | Audit de l'utilisation des fonctions privilégiées	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(9)	Moindre privilège AC-6 (9) | Audit de l'utilisation des fonctions privilégiées	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(9)	Moindre privilège AC-6 (9) | Audit de l'utilisation des fonctions privilégiées	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AC-6(9)	Moindre privilège AC-6 (9) | Audit de l'utilisation des fonctions privilégiées	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(9)	Moindre privilège AC-6 (9) | Audit de l'utilisation des fonctions privilégiées	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(9)	Moindre privilège AC-6 (9) | Audit de l'utilisation des fonctions privilégiées	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(10)	Moindre privilège AC-6(10) | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(10)	Moindre privilège AC-6(10) | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(10)	Moindre privilège AC-6(10) | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(10)	Moindre privilège AC-6(10) | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6(10)	Moindre privilège AC-6(10) | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées s qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-6.A	Moindre privilège AC-6.A	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(1)	Accès à distance AC-17 (1) | Surveillance/contrôle automatisés	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(2)	Accès à distance AC-17(2) | Protection de la confidentialité/l'intégrité à l'aide du chiffrement	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-AC-17(2)	Accès à distance AC-17(2) | Protection de la confidentialité/l'intégrité à l'aide du chiffrement	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(2)	Accès à distance AC-17(2) | Protection de la confidentialité/l'intégrité à l'aide du chiffrement	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(2)	Accès à distance AC-17(2) | Protection de la confidentialité/l'intégrité à l'aide du chiffrement	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-AC-17(2)	Accès à distance AC-17(2) | Protection de la confidentialité/ l'intégrité à l'aide du chiffrement	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(2)	Accès à distance AC-17(2) | Protection de la confidentialité/l'intégrité à l'aide du chiffrement	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(3)	Accès à distance AC-17(3) | Points de contrôle d'accès gérés	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(4)	Accès à distance AC-17(4) | Commandes/accès privilégiés	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(4)	Accès à distance AC-17(4) | Commandes/accès privilégiés	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17(4)	Accès à distance AC-17(4) | Commandes/accès privilégiés	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.A	Accès à distance AC-17.A	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.AA	Accès à distance AC-17.AA	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AC-17.B	Accès à distance AC-17.B	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.A	Événements d'audit AU-2.A	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.B	Événements d'audit AU-2.B	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.C	Événements d'audit AU-2.C	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-2.D	Événements d'audit AU-2.D	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3(1)	Contenu des enregistrements d'audit AU-3(1) | Informations d'audit supplémentaires	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-3.A	Contenu des enregistrements d'audit AU-3.A	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-5.A	Réponse aux échecs du traitement d'audit AU-5.A	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-5.B	Réponse aux échecs du traitement d'audit AU-5.B	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(1)	Examen, analyse et génération de rapports d'audit AU-6(1) | Intégration des processus	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(1)	Examen, analyse et génération de rapports d'audit AU-6(1) | Intégration des processus	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(1)	Examen, analyse et génération de rapports d'audit AU-6(1) | Intégration des processus	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(1)	Examen, analyse et génération de rapports d'audit AU-6(1) | Intégration des processus	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(1)	Examen, analyse et génération de rapports d'audit AU-6(1) | Intégration des processus	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-6(1)	Examen, analyse et génération de rapports d'audit AU-6(1) | Intégration des processus	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-6(3)	Examen, analyse et génération de rapports d'audit AU-6 (3) | Corréler les référentiels d'audit	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-7(1)	Réduction des audits et génération de rapports AU-7(1) | Traitement automatique	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-8.B	Horodatages AU-8.B	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-9(2)	Protection des informations d'audit AU-9(2) | Sauvegarde d'audit sur des systèmes/composants physiques distincts	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-AU-9(2)	Protection des informations d'audit AU-9(2) | Sauvegarde d'audit sur des systèmes/composants physiques distincts	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-9(2)	Protection des informations d'audit AU-9(2) | Sauvegarde d'audit sur des systèmes/composants physiques distincts	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-9.A	Protection des informations d'audit AU-9.A	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-9.A	Protection des informations d'audit AU-9.A	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-9.A	Protection des informations d'audit AU-9.A	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-11.A	Conservation des enregistrements d'audit AU-11.A	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-11.B	Conservation des enregistrements d'audit AU-11.B	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-11.C	Conservation des enregistrements d'audit AU-11.C	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.A	Génération d'audits AU-12.A	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-AU-12.C	Génération d'audits AU-12.C	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-3(5)	Interconnexions de systèmes CA-3(5) | Restrictions sur les connexions réseau externes	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.A	Surveillance continue CA-7.A	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.B	Surveillance continue CA-7.B	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.C	Surveillance continue CA-7.C	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.D	Surveillance continue CA-7.D	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.E	Surveillance continue CA-7.E	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.F	Surveillance continue CA-7.F	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	api-gw-xray-enabled	AWS X-Ray collecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation. Assurez-vous que X-Ray est activé afin que vous puissiez consulter des informations détaillées non seulement sur la demande et la réponse, mais également sur les appels que votre application fait aux AWS ressources en aval, aux microservices, aux bases de données et aux API Web HTTP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-7.G	Surveillance continue CA-7.G	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CA-9.A	Connexions au système interne CA-9.A	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-2.A	Configuration de référence CM-2.A	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-2.A	Configuration de référence CM-2.A	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-2.A	Configuration de référence CM-2.A	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-2.A	Configuration de référence CM-2.A	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-2.A	Configuration de référence CM-2.A	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-2.A	Configuration de référence CM-2.A	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-2.A	Configuration de référence CM-2.A	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.A	Contrôle des modifications de configuration CM-3.A	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.A	Contrôle des modifications de configuration CM-3.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-3.B	Contrôle des modifications de configuration CM-3.B	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.B	Contrôle des modifications de configuration CM-3.B	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-3.C	Contrôle des modifications de configuration CM-3.C	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.C	Contrôle des modifications de configuration CM-3.C	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-3.D	Contrôle des modifications de configuration CM-3.D	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.D	Contrôle des modifications de configuration CM-3.D	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-3.E	Contrôle des modifications de configuration CM-3.E	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.E	Contrôle des modifications de configuration CM-3.E	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-3.F	Contrôle des modifications de configuration CM-3F	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.F	Contrôle des modifications de configuration CM-3F	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-3.G	Contrôle des modifications de configuration CM-3.G	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-3.G	Contrôle des modifications de configuration CM-3.G	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(1)	Restrictions d'accès liées au changement CM-5(1) | Exécution/audit automatisés des accès	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5(5)	Restrictions d'accès liées au changement CM-5(5) | Limitation de la production/ Privilèges opérationnels	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-5.A	Restrictions d'accès liées au changement CM-5.A	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6(1)	Paramètres de configuration CM-6(1) | Gestion/application/vérification centralisées automatisées	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6(1)	Paramètres de configuration CM-6(1) | Gestion/application/vérification centralisées automatisées	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6(1)	Paramètres de configuration CM-6(1) | Gestion/application/vérification centralisées automatisées	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.A	Paramètres de configuration CM-6.A	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.B	Paramètres de configuration CM-6.B	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.C	Paramètres de configuration CM-6.C	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-6.D	Paramètres de configuration CM-6.D	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-7.A	Principe de moindre fonctionnalité CM-7.A	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-7.A	Principe de moindre fonctionnalité CM-7.A	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-7.B	Principe de moindre fonctionnalité CM-7.B	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-7.B	Principe de moindre fonctionnalité CM-7.B	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(1)	Inventaire des composants du système d'information CM-8(1) | Mises à jour lors de l'installation/la suppression	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(1)	Inventaire des composants du système d'information CM-8(1) | Mises à jour lors de l'installation/la suppression	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(2)	Inventaire des composants du système d'information CM-8(2) | Maintenance automatisée	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(2)	Inventaire des composants du système d'information CM-8(2) | Maintenance automatisée	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(3)	Inventaire des composants du système d'information CM-8(3) | Détection automatisée des composants non autorisés	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(3)	Inventaire des composants du système d'information CM-8(3) | Détection automatisée des composants non autorisés	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(3)	Inventaire des composants du système d'information CM-8(3) | Détection automatisée des composants non autorisés	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8(3)	Inventaire des composants du système d'information CM-8(3) | Détection automatisée des composants non autorisés	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.A	Inventaire des composants du système d'information CM-8.A	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.A	Inventaire des composants du système d'information CM-8.A	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.B	Inventaire des composants du système d'information CM-8.B	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.B	Inventaire des composants du système d'information CM-8.B	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.C	Inventaire des composants du système d'information CM-8.C	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.C	Inventaire des composants du système d'information CM-8.C	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.D	Inventaire des composants du système d'information CM-8.D	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.D	Inventaire des composants du système d'information CM-8.D	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.E	Inventaire des composants du système d'information CM-8.E	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CM-8.E	Inventaire des composants du système d'information CM-8.E	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relationa l Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(5)	Plan d'urgence CP-2(5) | Poursuivre les missions/fonctions métier essentielles	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(6)	Plan d'urgence CP-2(6) | Site de traitement/stockage alternatif	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(6)	Plan d'urgence CP-2(6) | Site de traitement/stockage alternatif	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(6)	Plan d'urgence CP-2(6) | Site de traitement/stockage alternatif	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CP-2(6)	Plan d'urgence CP-2(6) | Site de traitement/stockage alternatif	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relationa l Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(6)	Plan d'urgence CP-2(6) | Site de traitement/stockage alternatif	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2(6)	Plan d'urgence CP-2(6) | Site de traitement/stockage alternatif	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relationa l Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.A	Plan d'urgence CP-2.A	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.B	Plan d'urgence CP-2.B	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.C	Plan d'urgence CP-2.C	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.D	Plan d'urgence CP-2.D	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.E	Plan d'urgence CP-2.E	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relationa l Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.F	Plan d'urgence CP-2.F	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relationa l Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-2.G	Plan d'urgence CP-2.G	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(1)	Site de stockage alternatif CP-6(1) | Séparation du site principal	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6(2)	Site de stockage alternatif CP-6(2) | Objectifs en matière de délai et de point de récupération	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.A	Site de stockage alternatif CP-6.A	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-6.B	Site de stockage alternatif CP-6.B	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(3)	Sauvegarde du système d'information CP-9(3) | Stockage séparé pour les informations critiques	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(7)	Sauvegarde du système d'information CP-9(7) | Double autorisation	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9(7)	Sauvegarde du système d'information CP-9(7) | Double autorisation	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.A	Sauvegarde du système d'information CP-9.A	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.AA	Sauvegarde du système d'information CP-9.AA	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.B	Sauvegarde du système d'information CP-9.B	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.C	Sauvegarde du système d'information CP-9.C	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-9.D	Sauvegarde du système d'information CP-9.D	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-CP-10.A	Reprise et reconstitution du système d'information CP-10.A	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(1)	Identification et authentification (utilisateurs de l'organisation) IA-2(1) | Accès réseau aux comptes privilégiés	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(1)	Identification et authentification (utilisateurs de l'organisation) IA-2(1) | Accès réseau aux comptes privilégiés	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(1)	Identification et authentification (utilisateurs de l'organisation) IA-2(1) | Accès réseau aux comptes privilégiés	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(3)	Identification et authentification (utilisateurs de l'organisation) IA-2(3) | Accès local aux comptes privilégiés	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(3)	Identification et authentification (utilisateurs de l'organisation) IA-2(3) | Accès local aux comptes privilégiés	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(3)	Identification et authentification (utilisateurs de l'organisation) IA-2(3) | Accès local aux comptes privilégiés	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(8)	Identification et authentification (utilisateurs de l'organisation) IA-2(8) | Accès réseau aux comptes privilégi és - résistant aux réexécutions	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(8)	Identification et authentification (utilisateurs de l'organisation) IA-2(8) | Accès réseau aux comptes privilégi és - résistant aux réexécutions	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(8)	Identification et authentification (utilisateurs de l'organisation) IA-2(8) | Accès réseau aux comptes privilégi és - résistant aux réexécutions	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(11)	Identification et authentification (utilisateurs de l'organisation) IA-2(11) | Accès à distancer - appareil distinct	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(11)	Identification et authentification (utilisateurs de l'organisation) IA-2(11) | Accès à distancer - appareil distinct	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2(11)	Identification et authentification (utilisateurs de l'organisation) IA-2(11) | Accès à distancer - appareil distinct	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2.A	Identification et authentification (utilisateurs de l'organisation) IA-2.A	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2.A	Identification et authentification (utilisateurs de l'organisation) IA-2.A	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2.A	Identification et authentification (utilisateurs de l'organisation) IA-2.A	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-2.A	Identification et authentification (utilisateurs de l'organisation) IA-2.A	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4(4)	Gestion des identifiants IA-4(4) | Identifier le statut d'utilisateur	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.A	Gestion des identifiants IA-4.A	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.A	Gestion des identifiants IA-4.A	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.A	Gestion des identifiants IA-4.A	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.B	Gestion des identifiants IA-4.B	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.B	Gestion des identifiants IA-4.B	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.B	Gestion des identifiants IA-4.B	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.C	Gestion des identifiants IA-4.C	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.C	Gestion des identifiants IA-4.C	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.C	Gestion des identifiants IA-4.C	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.D	Gestion des identifiants IA-4.D	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.D	Gestion des identifiants IA-4.D	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.D	Gestion des identifiants IA-4.D	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.E	Gestion des identifiants IA-4.E	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.E	Gestion des identifiants IA-4.E	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-4.E	Gestion des identifiants IA-4.E	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5(1)	Gestion des authentif icateurs IA-5(1) | Authentification par mot de passe	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5(2)	Gestion des authentif icateurs IA-5(2) | Authentification par PKI	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5(2)	Gestion des authentif icateurs IA-5(2) | Authentification par PKI	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5(4)	Gestion des authentif icateurs IA-5(4) | Prise en charge automatis ée de la détermina tion de la sécurité des mots de passe	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5(8)	Gestion des authentif icateurs IA-5(8) | Comptes de plusieurs systèmes d'informa tion	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5(8)	Gestion des authentif icateurs IA-5(8) | Comptes de plusieurs systèmes d'informa tion	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5(8)	Gestion des authentif icateurs IA-5(8) | Comptes de plusieurs systèmes d'informa tion	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.A	Gestion des authentif icateurs IA-5.A	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.A	Gestion des authentif icateurs IA-5.A	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.A	Gestion des authentif icateurs IA-5.A	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.A	Gestion des authentif icateurs IA-5.A	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.B	Gestion des authentif icateurs IA-5.B	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.B	Gestion des authentif icateurs IA-5.B	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.B	Gestion des authentif icateurs IA-5.B	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.B	Gestion des authentif icateurs IA-5.B	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.C	Gestion des authentif icateurs IA-5.C	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.C	Gestion des authentif icateurs IA-5.C	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.C	Gestion des authentif icateurs IA-5.C	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.C	Gestion des authentif icateurs IA-5.C	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.D	Gestion des authentif icateurs IA-5.D	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.D	Gestion des authentif icateurs IA-5.D	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.D	Gestion des authentif icateurs IA-5.D	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.D	Gestion des authentif icateurs IA-5.D	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.E	Gestion des authentif icateurs IA-5.E	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.E	Gestion des authentif icateurs IA-5.E	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.E	Gestion des authentif icateurs IA-5.E	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.E	Gestion des authentif icateurs IA-5.E	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.F	Gestion des authentif icateurs IA-5.F	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.F	Gestion des authentif icateurs IA-5.F	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.F	Gestion des authentif icateurs IA-5.F	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.F	Gestion des authentif icateurs IA-5.F	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.G	Gestion des authentif icateurs IA-5.G	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.G	Gestion des authentif icateurs IA-5.G	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.G	Gestion des authentif icateurs IA-5.G	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.G	Gestion des authentif icateurs IA-5.G	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.H	Gestion des authentif icateurs IA-5.H	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.H	Gestion des authentif icateurs IA-5.H	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.H	Gestion des authentif icateurs IA-5.H	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.H	Gestion des authentif icateurs IA-5.H	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.l	Gestion des authentif icateurs IA-5.l	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.l	Gestion des authentif icateurs IA-5.l	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.I	Gestion des authentif icateurs IA-5.I	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.I	Gestion des authentif icateurs IA-5.I	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.J	Gestion des authentif icateurs IA-5.J	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.J	Gestion des authentif icateurs IA-5.J	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.J	Gestion des authentif icateurs IA-5.J	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IA-5.J	Gestion des authentif icateurs IA-5.J	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-IR-6(1)	Signalement des incidents IR-6(1) | Génération de rapports automatisés	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-3.A	Outils de maintenance MA-3.A	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-3.A	Outils de maintenance MA-3.A	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MA-4(1)	Maintenance non locale MA-4(1) | Audit et révision	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-MP-2.A	Accès média MP-2.A	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-RA-5.A	Analyse des vulnérabilités RA-5.A	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-RA-5.B	Analyse des vulnérabilités RA-5.B	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-RA-5.C	Analyse des vulnérabilités RA-5.C	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-RA-5.D	Analyse des vulnérabilités RA-5.D	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-RA-5.E	Analyse des vulnérabilités RA-5.E	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SA-10(1)	Gestion de la configuration pour les développeurs SA-10(1) | Vérification de l'intégrité du logiciel/microprogramme	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-5.A	Protection contre le déni de service SC-5.A	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-5.A	Protection contre le déni de service SC-5.A	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relationa l Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-6.A	Disponibilité des ressources SC-6.A	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(3)	Protection des limites SC-7(3) | Points d'accès	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(4)	Protection des limites SC-7(4) | Services de télécommunications externes	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(5)	Protection des limites SC-7(5) | Rejeter par défaut/autoriser par exception	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(5)	Protection des limites SC-7(5) | Rejeter par défaut/autoriser par exception	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(5)	Protection des limites SC-7(5) | Rejeter par défaut/autoriser par exception	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(5)	Protection des limites SC-7(5) | Rejeter par défaut/autoriser par exception	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7(7)	Protection des limites SC-7(7) | Empêcher le split tunneling pour les appareils distants	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.A	Protection des limites SC-7.A	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.B	Protection des limites SC-7.B	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-7.C	Protection des limites SC-7.C	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8(1)	Intégrité et confident ialité des transmiss ions SC-8(1) | Protection par le chiffrement ou autre protection physique	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-8(1)	Intégrité et confident ialité des transmiss ions SC-8(1) | Protection par le chiffrement ou autre protection physique	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8(1)	Intégrité et confident ialité des transmiss ions SC-8(1) | Protection par le chiffrement ou autre protection physique	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8(1)	Intégrité et confidentialité des transmissions SC-8(1) | Protection par le chiffrement ou autre protection physique	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8(1)	Intégrité et confidentialité des transmissions SC-8(1) | Protection par le chiffrement ou autre protection physique	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-SC-8(1)	Intégrité et confidentialité des transmissions SC-8(1) | Protection par le chiffrement ou autre protection physique	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8(1)	Intégrité et confidentialité des transmissions SC-8(1) | Protection par le chiffrement ou autre protection physique	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-8(1)	Intégrité et confidentialité des transmissions SC-8(1) | Protection par le chiffrement ou autre protection physique	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8(1)	Intégrité et confidentialité des transmissions SC-8(1) | Protection par le chiffrement ou autre protection physique	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-8.A	Confidentialité et intégrité des transmissions SC-8.A	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-12(1)	Établissement et gestion des clés de chiffrement SC-12(1) | Disponibilité	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
CCCS-fPBMM-SC-12(2)	Établissement et gestion des clés de chiffrement SC-12(2) | Clés symétriques	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-12(2)	Établissement et gestion des clés de chiffrement SC-12(2) | Clés symétriques	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
CCCS-fPBMM-SC-12.A	Établissement et gestion des clés de chiffrement SC-12.A	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-12.A	Établissement et gestion des clés de chiffrement SC-12.A	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-13.A	Protection par le chiffrement SC-13.A	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-22.A	Architecture et mise en service du service de résolution de noms/d'adresses SC-22.A	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-23.A	Authenticité des sessions SC-23.A	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28(1)	Protection des informations au repos SC-28(1) | Protection par le chiffrement	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SC-28.A	Protection des informations au repos SC-28.A	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatiq ue des failles	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatiq ue des failles	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrast ructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibi lité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournisse nt un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatique des failles	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatique des failles	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatiq ue des failles	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatiq ue des failles	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatique des failles	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatique des failles	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatiq ue des failles	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environne ment Amazon Elastic Beanstalk garantit l'installation des derniers correctif s, mises à jour et fonctionnalités de la plateforme disponibl es pour l'environ nement. La sécurisat ion des systèmes passe par la mise à jour de l'installation des correctifs.
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatiq ue des failles	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatique des failles	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(2)	Correction des failles SI-2(2) | État de la correction automatique des failles	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2(3)	Correction des failles SI-2(3) | Délai pour remédier aux failles/ critères de référence pour les mesures correctives	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.A	Correction des failles SI-2.A	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.B	Correction des failles SI-2.B	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.C	Correction des failles SI-2.C	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-2.D	Correction des failles SI-2.D	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3(1)	Protection contre les codes malveillants SI-3(1) | Gestion centrale	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3(7)	Protection contre les codes malveillants SI-3(7) | Détection non basée sur les signatures	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.A	Protection contre les codes malveillants SI-3.A	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.A	Protection contre les codes malveillants SI-3.A	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.A	Protection contre les codes malveillants SI-3.A	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.A	Protection contre les codes malveillants SI-3.A	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.A	Protection contre les codes malveillants SI-3.A	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.B	Protection contre les codes malveillants SI-3.B	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.B	Protection contre les codes malveillants SI-3.B	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.B	Protection contre les codes malveillants SI-3.B	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.B	Protection contre les codes malveillants SI-3.B	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.C	Protection contre les codes malveillants SI-3.C	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.C	Protection contre les codes malveillants SI-3.C	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.C	Protection contre les codes malveillants SI-3.C	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.C	Protection contre les codes malveillants SI-3.C	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.D	Protection contre les codes malveillants SI-3.D	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.D	Protection contre les codes malveillants SI-3.D	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.D	Protection contre les codes malveillants SI-3.D	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-3.D	Protection contre les codes malveillants SI-3.D	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(1)	Surveillance du système d'information SI-4(1) | Système de détection des intrusions à l'échelle du système	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(1)	Surveillance du système d'informa tion SI-4(1) | Système de détection des intrusions à l'échelle du système	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(2)	Surveillance du système d'information SI-4(2) | Outils automatisés pour l'analyse en temps réel	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(2)	Surveillance du système d'information SI-4(2) | Outils automatisés pour l'analyse en temps réel	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(4)	Surveillance du système SI-4(4) | Trafic des communications entrantes et sortantes	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(4)	Surveillance du système SI-4(4) | Trafic des communications entrantes et sortantes	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(5)	Surveillance du système d'information SI-4(5) | Alertes générées par le système	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(11)	Surveillance du système d'information SI-4(11) | Analyser les anomalies du trafic des communications	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(11)	Surveillance du système d'information SI-4(11) | Analyser les anomalies du trafic des communications	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(16)	Surveillance du système d'information SI-4(16) | Corréler les informations de surveillance	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(16)	Surveillance du système d'information SI-4(16) | Corréler les informations de surveillance	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(20)	Surveillance du système d'information SI-4(20) | Utilisateur privilégié	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(23)	Surveillance du système d'information SI-4(23) | Appareils basés sur l'hôte	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4(23)	Surveillance du système d'information SI-4(23) | Appareils basés sur l'hôte	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CCCS-fPBMM-SI-4.A	Surveillance du système d'information SI-4.A	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.A	Surveillance du système d'information SI-4.A	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.A	Surveillance du système d'information SI-4.A	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
CCCS-fPBMM-SI-4.A	Surveillance du système d'information SI-4.A	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.A	Surveillance du système d'information SI-4.A	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.B	Surveillance du système d'information SI-4.B	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.B	Surveillance du système d'information SI-4.B	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.B	Surveillance du système d'information SI-4.B	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
CCCS-fPBMM-SI-4.B	Surveillance du système d'information SI-4.B	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.B	Surveillance du système d'information SI-4.B	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.C	Surveillance du système d'information SI-4.C	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.C	Surveillance du système d'information SI-4.C	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.C	Surveillance du système d'information SI-4.C	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
CCCS-fPBMM-SI-4.C	Surveillance du système d'information SI-4.C	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.C	Surveillance du système d'information SI-4.C	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.D	Surveillance du système d'information SI-4.D	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.D	Surveillance du système d'information SI-4.D	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.D	Surveillance du système d'information SI-4.D	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
CCCS-fPBMM-SI-4.D	Surveillance du système d'information SI-4.D	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.D	Surveillance du système d'information SI-4.D	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.E	Surveillance du système d'information SI-4.E	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.E	Surveillance du système d'information SI-4.E	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.E	Surveillance du système d'information SI-4.E	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
CCCS-fPBMM-SI-4.E	Surveillance du système d'information SI-4.E	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.E	Surveillance du système d'information SI-4.E	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.F	Surveillance du système d'information SI-4.F	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.F	Surveillance du système d'information SI-4.F	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.F	Surveillance du système d'information SI-4.F	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
CCCS-fPBMM-SI-4.F	Surveillance du système d'information SI-4.F	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.F	Surveillance du système d'information SI-4.F	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.G	Surveillance du système d'information SI-4.G	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.G	Surveillance du système d'information SI-4.G	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.G	Surveillance du système d'information SI-4.G	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
CCCS-fPBMM-SI-4.G	Surveillance du système d'information SI-4.G	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-4.G	Surveillance du système d'information SI-4.G	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-5.A	Alertes, conseils et directives de sécurité SI-5.A	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-5.B	Alertes, conseils et directives de sécurité SI-5.B	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-5.C	Alertes, conseils et directives de sécurité SI-5.C	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-5.D	Alertes, conseils et directives de sécurité SI-5.D	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-7(1)	Intégrité des logiciels, des microprogrammes et des informations SI-7(1) | Contrôles d'intégrité	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-7(7)	Intégrité des logiciels, des microprogrammes et des informations SI-7(7) | Intégration de la détection et de la réponse	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-7.A	Intégrité des logiciels, des microprogrammes et des informations SI-7.A	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CCCS-fPBMM-SI-12.A	Gestion et conservation des informations SI-12.A	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour le profil moyen de contrôle du cloud du Centre canadien pour la cybersécurité (CCCS).

Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 1

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité

spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 1 et les règles de AWS Config/Process Checks AWS Config gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CIS Amazon Web Services Foundation v1.4 de niveau 1. Un contrôle CIS Amazon Web Services Foundation v1.4 de niveau 1 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Pour plus d'informations sur les vérifications de processus, consultez process-checks.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Conserver les informations de contact actuelles	account-contact-details-configured (vérification du processus)	Assurez-vous que l'adresse e-mail et le numéro de téléphone des comptes AWS sont à jour et correspon dent à plusieurs personnes au sein de votre organisation. Dans la section Mon compte de la console, assurez-vous que les informations correctes sont spécifiées dans la section Informati ons de contact. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/
1.2	Vérifier que les informations de contact de sécurité sont enregistrées	account-security-contact-configured (Vérification du processus)	Assurez-vous que l'adresse e-mail et le numéro de téléphone de l'équipe de sécurité de votre organisation sont à jour. Dans la section Mon compte de la console de AWS gestion, assurez-vous que les informations correctes sont spécifiées dans la section Sécurité. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.4	Vérifier qu'il n'existe aucune clé d'accès d'utilisateur root	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.5	Vérifier que la MFA est activée pour l'utilisateur root	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,7	Éliminer le recours à l'utilisateur root pour les tâches administr atives et quotidiennes	root-account-regular-use (Vérification du processus)	Veillez à ce que le compte root ne soit pas utilisé pour les tâches quotidiennes. Dans IAM, exécutez un rapport sur les informations d'identif ication pour vérifier quand l'utilisateur root a été utilisé pour la dernière fois. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.8	Vérifier que la politique de mot de passe IAM exige un mot de passe d'au moins 14 caractères	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.9	Vérifier que la politique de mot de passe IAM empêche la réutilisation d'un mot de passe	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.10	Vérifier que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs dotés d'un mot de passe de console	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.11	Ne pas configurer des clés d'accès au cours de la configuration initiale de tous les utilisateurs qui ont un mot de passe de console	iam-user-console-and- (vérification du processus) api-access-at-creation	Vérifiez qu'aucune clé d'accès n'est configurée au cours de la configuration initiale de tous les utilisateurs qui ont un mot de passe de console. Pour tous les utilisateurs ayant accès à la console, comparez l'heure de création de l'utilisateur à la date de création de la clé d'accès. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.12	Vérifier que les informations d'identification inutilisées depuis 45 jours ou plus sont désactivées	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir l'maxCredentialUsageâge (valeur standard CIS : 45). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.13	Vérifier qu'une seule clé d'accès active est disponible pour chaque utilisateur	iam- user-single-access-key (Vérification du processus)	Vérifiez qu'une seule clé d'accès active est disponible pour chaque utilisateur. Pour chaque utilisateur IAM, vérifiez qu'une seule clé active est utilisée dans l'onglet Informations d'identification de sécurité. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.14	Vérifier que les clés d'accès font l'objet d'une rotation tous les 90 jours maximum	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.15	Vérifier que les utilisateurs reçoivent des autorisations uniquement par le biais de groupes	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.15	Vérifier que les utilisateurs reçoivent des autorisations uniquement par le biais de groupes	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.15	Vérifier que les utilisateurs reçoivent des autorisations uniquement par le biais de groupes	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.16	Vérifier qu'aucune politique IAM autorisant des privilèges d'administrateur « *:* » complets n'est jointe	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,17	Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avec AWS Support	iam-policy-in-use	AWS Identity and Access Management (IAM) peut vous aider à gérer les autorisations et autorisations d'accès en veillant à ce que les politiques IAM soient attribuées aux utilisateurs, rôles ou groupes appropriés. La restriction de ces politiques intègre également les principes du moindre privilège et de la séparation des tâches. Cette règle nécessite que vous définissiez le PolicYarn sur arn:aws:iam : :aws:policy/, pour la gestion des incidents avec Support. AWSSupportAccess AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,19	Vérifier que tous les certificats SSL/TLS expirés stockés dans AWS IAM sont supprimés	iam-expired-certificates (Vérification du processus)	Vérifiez que tous les certificats SSL/TLS expirés stockés dans IAM sont supprimés. À partir de la ligne de commande avec la AWS CLI installée, exécutez la commande « AWS iam list-server-certificates » et déterminez s'il existe des certificats de serveur expirés. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,20	Assurez-vous que l'analyseur d'accès AWS IAM est activé	iam-access-analyzer-enabled (Vérification du processus)	Vérifiez que l'analyseur d'accès IAM est activé. Dans la section IAM de la console, sélectionnez Analyseur d'accès et assurez-vous que le STATUT est défini sur Actif. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1.3	Vérifier que la suppression MFA est activée sur les compartiments S3	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. L'ajout de la suppression par authentification multifactorielle (MFA) à un compartiment S3 nécessite un facteur d'authentification supplémentaire afin de modifier l'état de version de votre compartiment ou de supprimer une version d'objet. La suppressi on MFA peut ajouter un niveau de sécurité supplémentaire en cas d'informations d'identification de sécurité compromises ou d'octroi d'un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1.5	Vérifier que « Bloquer l'accès public (paramètres de compartiment) » est défini pour les compartiments S3	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1.5	Vérifier que « Bloquer l'accès public (paramètres de compartiment) » est défini pour les compartiments S3	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
2.2.1	Vérifier que le chiffrement de volume EBS est activé	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.1	Vérifier que le chiffrement de volume EBS est activé	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
2.3.1	Vérifier que le chiffrement est activé pour les instances RDS	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.3.1	Vérifier que le chiffrement est activé pour les instances RDS	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1	Assurez-vous qu' CloudTrail il est activé dans toutes les régions	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.3	Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
3.4	Assurez-vous que les CloudTrail sentiers sont intégrés aux CloudWatch journaux	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6	Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les appels d'API non autorisés	alarm-unauthorized-api-calls (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les appels d'API non autorisés. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.2	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour la connexion à la console de gestion sans MFA	alarm- sign-in-without-mfa (vérification du processus)	Assurez-vous qu'un filtre de métrique de journaux et une alarme existent pour la connexion à la console de gestion AWS sans authentification multifactorielle (MFA). Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3	Vérifier qu'il existe un filtre de métrique de journaux et une alarme en cas d'utilisation du compte root	alarm-root-account-use (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme en cas d'utilisation du compte root. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,4	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique IAM	alarm-iam-policy-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique IAM. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,5	Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modificat ions CloudTrail de configuration	alarm-cloudtrail-c onfig-change (Vérifica tion du processus)	Assurez-vous qu'un filtre logarithmique et qu'une alarme existent pour les modifications AWS CloudTrail de configuration. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique de compartiment S3	alarm-s3- bucket-policy-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique de compartiment S3. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,12	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des passerelles réseau	alarm- vpc-network-gateway-change (vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des passerelles réseau. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,13	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des tables de routage	alarm- vpc-route-table-change (vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des tables de routage. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,14	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications VPC	alarm-vpc-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications Amazon Virtual Private Cloud (VPC). Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,15	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications AWS Organizations	alarm-organizations-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications AWS Organizations. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.1	Vérifier qu'aucune liste ACL réseau n'autorise l'entrée depuis 0.0.0.0/0 vers des ports d'adminis tration de serveur distant	nacl-no-unrestricted-ssh-rdp	Vérifiez qu'aucune liste ACL réseau n'autorise l'entrée publique vers les ports d'adminis tration de serveur distant. Dans la section VPC de la console, assurez-vous qu'il n'existe pas d'ACL réseau avec une source « 0.0.0.0/0 » autorisan t des ports ou des plages de ports incluant des ports d'administration de serveur distant. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Vérifier qu'aucun groupe de sécurité n'autorise l'entrée depuis 0.0.0.0/0 vers des ports d'adminis tration de serveur distant	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Vérifier qu'aucun groupe de sécurité n'autorise l'entrée depuis 0.0.0.0/0 vers des ports d'adminis tration de serveur distant	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet de définir éventuell ement les paramètre s blockedPort1 à blockedPort5 (valeur standard CIS : 3389). Les valeurs réelles doivent refléter les politiques de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 1.

Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 2

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 2 et les règles de AWS Config/Process Checks AWS Config gérés. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CIS Amazon Web Services Foundation v1.4 de niveau 2. Un contrôle CIS Amazon Web Services Foundation v1.4 de niveau 2 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Pour plus d'informations sur les vérifications de processus, consultez process-checks.

Région AWS: partout Régions AWS où les packs de conformité sont pris en charge (support régional) sauf AWS GovCloud (États-Unis Est), AWS GovCloud (États-Unis Ouest) et Moyen-Orient (Bahreïn)

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Conserver les informations de contact actuelles	account-contact-details-configured (vérification du processus)	Assurez-vous que l'adresse e-mail et le numéro de téléphone des comptes AWS sont à jour et correspon dent à plusieurs personnes au sein de votre organisation. Dans la section Mon compte de la console,

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			assurez-vous que les informations correctes sont spécifiées dans la section Informations de contact. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2	Vérifier que les informations de contact de sécurité sont enregistrées	account-security-contact-configured (Vérification du processus)	Assurez-vous que l'adresse e-mail et le numéro de téléphone de l'équipe de sécurité de votre organisation sont à jour. Dans la section Mon compte de la console de AWS gestion, assurez-vous que les informations correctes sont spécifiées dans la section Sécurité. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.4	Vérifier qu'il n'existe aucune clé d'accès d'utilisateur root	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.5	Vérifier que la MFA est activée pour l'utilisateur root	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.6	Vérifier que la MFA matérielle est activée pour le compte d'utilisateur root	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,7	Éliminer le recours à l'utilisateur root pour les tâches administr atives et quotidiennes	root-account-regular-use (Vérification du processus)	Veillez à ce que le compte root ne soit pas utilisé pour les tâches quotidiennes. Dans IAM, exécutez un rapport sur les informations d'identif ication pour vérifier quand l'utilisateur root a été utilisé pour la dernière fois. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.8	Vérifier que la politique de mot de passe IAM exige un mot de passe d'au moins 14 caractères	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.9	Vérifier que la politique de mot de passe IAM empêche la réutilisation d'un mot de passe	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.10	Vérifier que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs dotés d'un mot de passe de console	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.11	Ne pas configurer des clés d'accès au cours de la configuration initiale de tous les utilisateurs qui ont un mot de passe de console	iam-user-console-and- (vérification du processus) api-access-at-creation	Vérifiez qu'aucune clé d'accès n'est configurée au cours de la configuration initiale de tous les utilisateurs qui ont un mot de passe de console. Pour tous les utilisateurs ayant accès à la console, comparez l'heure de création de l'utilisateur à la date de création de la clé d'accès. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.12	Vérifier que les informations d'identification inutilisées depuis 45 jours ou plus sont désactivées	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir l'maxCredentialUsageâge (valeur standard CIS : 45). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.13	Vérifier qu'une seule clé d'accès active est disponible pour chaque utilisateur	iam- user-single-access-key (Vérification du processus)	Vérifiez qu'une seule clé d'accès active est disponible pour chaque utilisateur. Pour chaque utilisateur IAM, vérifiez qu'une seule clé active est utilisée dans l'onglet Informations d'identification de sécurité. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.14	Vérifier que les clés d'accès font l'objet d'une rotation tous les 90 jours maximum	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.15	Vérifier que les utilisateurs reçoivent des autorisations uniquement par le biais de groupes	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.15	Vérifier que les utilisateurs reçoivent des autorisations uniquement par le biais de groupes	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.15	Vérifier que les utilisateurs reçoivent des autorisations uniquement par le biais de groupes	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.16	Vérifier qu'aucune politique IAM autorisant des privilèges d'administrateur « *:* » complets n'est jointe	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,17	Assurez-vous qu'un rôle de support a été créé pour gérer les incidents avec AWS Support	iam-policy-in-use	AWS Identity and Access Management (IAM) peut vous aider à gérer les autorisations et autorisations d'accès en veillant à ce que les politiques IAM soient attribuées aux utilisateurs, rôles ou groupes appropriés. La restriction de ces politiques intègre également les principes du moindre privilège et de la séparation des tâches. Cette règle nécessite que vous définissiez le PolicYarn sur arn:aws:iam : :aws:policy/, pour la gestion des incidents avec Support. AWSSupportAccess AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,18	Assurez-vous que les rôles d'instance IAM sont utilisés pour l'accès aux AWS ressources à partir des instances	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,19	Vérifier que tous les certificats SSL/TLS expirés stockés dans AWS IAM sont supprimés	iam-expired-certificates (Vérification du processus)	Vérifiez que tous les certificats SSL/TLS expirés stockés dans IAM sont supprimés. À partir de la ligne de commande avec la AWS CLI installée, exécutez la commande « AWS iam list-server-certificates » et déterminez s'il existe des certificats de serveur expirés. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,20	Assurez-vous que l'analyseur d'accès AWS IAM est activé	iam-access-analyzer-enabled (Vérification du processus)	Vérifiez que l'analyseur d'accès IAM est activé. Dans la section IAM de la console, sélectionnez Analyseur d'accès et assurez-vous que le STATUT est défini sur Actif. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1,21	Assurez-vous que les utilisateurs sont gérés de manière centralisée via la fédération des identités ou AWS Organizations pour les environnements multi-comptes	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
2.1.1	Assurez-vous que tous les compartiments S3 utilisent encryption-at-rest	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1.2	Vérifier que la politique de compartiment S3 est définie de manière à refuser les requêtes HTTP	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1.3	Vérifier que la suppression MFA est activée sur les compartiments S3	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. L'ajout de la suppression par authentification multifactorielle (MFA) à un compartiment S3 nécessite un facteur d'authentification supplémentaire afin de modifier l'état de version de votre compartiment ou de supprimer une version d'objet. La suppressi on MFA peut ajouter un niveau de sécurité supplémentaire en cas d'informations d'identification de sécurité compromises ou d'octroi d'un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1.5	Vérifier que « Bloquer l'accès public (paramètres de compartiment) » est défini pour les compartiments S3	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1.5	Vérifier que « Bloquer l'accès public (paramètres de compartiment) » est défini pour les compartiments S3	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
2.2.1	Vérifier que le chiffrement de volume EBS est activé	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.1	Vérifier que le chiffrement de volume EBS est activé	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
2.3.1	Vérifier que le chiffrement est activé pour les instances RDS	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.3.1	Vérifier que le chiffrement est activé pour les instances RDS	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1	Assurez-vous que CloudTrail c'est activé dans toutes les régions	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.2	Assurez-vous que la validation du fichier CloudTrail journal est activée	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.3	Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Assurez-vous que le compartiment S3 utilisé pour stocker CloudTrail les journaux n'est pas accessible au public	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
3.4	Assurez-vous que les CloudTrail sentiers sont intégrés aux CloudWatch journaux	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,5	Assurez-vous que AWS Config est activé dans toutes les régions	config-enabled-all-regions (Vérification du processus)	Assurez-vous que AWS Config est activé dans toutes les AWS régions. Dans la section AWS Config de la console, pour chaque région activée, assurez-v ous que l'enregistreur de AWS configura tion est correctement configuré. Assurez-vous que l'enregis trement des ressource s AWS globales est activé dans au moins une région. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6	Assurez-vous que la journalisation des accès au compartiment S3 est activée sur le compartiment CloudTrail S3	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.7	Assurez-vous que CloudTrail les journaux sont chiffrés au repos à l'aide des CMK KMS	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
3.8	Vérifier que la rotation des clés CMK créées par le client est activée	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.9	Vérifier que la journalisation de flux VPC est activée dans tous les réseaux VPC	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
3,10	Vérifier que la journalisation au niveau de l'objet pour les événements d'écriture est activée pour le compartiment S3	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Vérifier que la journalisation au niveau de l'objet pour les événements de lecture est activée pour le compartiment S3	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
4.1	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les appels d'API non autorisés	alarm-unauthorized-api-calls (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les appels d'API non autorisés. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.2	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour la connexion à la console de gestion sans MFA	alarm- sign-in-without-mfa (vérification du processus)	Assurez-vous qu'un filtre de métrique de journaux et une alarme existent pour la connexion à la console de gestion AWS sans authentification multifactorielle (MFA). Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3	Vérifier qu'il existe un filtre de métrique de journaux et une alarme en cas d'utilisation du compte root	alarm-root-account-use (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme en cas d'utilisation du compte root. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,4	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique IAM	alarm-iam-policy-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique IAM. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,5	Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modificat ions CloudTrail de configuration	alarm-cloudtrail-c onfig-change (Vérifica tion du processus)	Assurez-vous qu'un filtre logarithmique et qu'une alarme existent pour les modifications AWS CloudTrail de configuration. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les échecs d'authent ification à la console de gestion AWS	alarm-console-auth-failures (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les échecs d'authent ification à la console de gestion AWS . Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,7	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour la désactivation ou la suppression planifiée des clés CMK créées par le client	alarm-kms- disable-or-delete-cmk (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour la désactivation ou la suppression planifiée des clés CMK créées par le client. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique de compartiment S3	alarm-s3- bucket-policy-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications de politique de compartiment S3. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,9	Assurez-vous qu'un journal, un filtre métrique et une alarme existent pour les modifications de configuration de AWS Config	alarm-aws-config-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications AWS Config. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,10	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des groupes de sécurité	alarm- vpc-secrity-group-change (vérification du processus)	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des groupes de sécurité. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,11	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des listes de contrôle d'accès réseau (ACL réseau)	alarm-vpc-nacl-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des listes de contrôle d'accès réseau (ACL réseau). Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,12	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des passerelles réseau	alarm- vpc-network-gateway-change (vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des passerelles réseau. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,13	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des tables de routage	alarm- vpc-route-table-change (vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications des tables de routage. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,14	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications VPC	alarm-vpc-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications Amazon Virtual Private Cloud (VPC). Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,15	Vérifier qu'il existe un filtre de métrique de journaux et une alarme pour les modifications AWS Organizations	alarm-organizations-change (Vérification du processus)	Vérifiez qu'il existe un filtre de métrique de journaux et une alarme pour les modifications AWS Organizations. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundations Benchmark version 1.4.0 disponible à l'adresse https://www.cisecurity.org/benchmark/amazon_web_services/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.1	Vérifier qu'aucune liste ACL réseau n'autorise l'entrée depuis 0.0.0.0/0 vers des ports d'adminis tration de serveur distant	nacl-no-unrestricted-ssh-rdp	Vérifiez qu'aucune liste ACL réseau n'autorise l'entrée publique vers les ports d'adminis tration de serveur distant. Dans la section VPC de la console, assurez-vous qu'il n'existe pas d'ACL réseau avec une source « 0.0.0.0/0 » autorisan t des ports ou des plages de ports incluant des ports d'administration de serveur distant. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Vérifier qu'aucun groupe de sécurité n'autorise l'entrée depuis 0.0.0.0/0 vers des ports d'adminis tration de serveur distant	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Vérifier qu'aucun groupe de sécurité n'autorise l'entrée depuis 0.0.0.0/0 vers des ports d'adminis tration de serveur distant	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet de définir éventuell ement les paramètre s blockedPort1 à blockedPort5 (valeur standard CIS : 3389). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.3	Vérifier que le groupe de sécurité par défaut de chaque réseau VPC restreint l'ensemble du trafic	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Vérifier que les tables de routage pour l'appairage de réseaux VPC ont un accès minimum	vpc-peering-least-access (Vérification du processus)	Vérifiez que les tables de routage pour l'appairage de réseaux VPC ont un accès minimum. Dans la section VPC de la console, examinez les entrées des tables de routage pour vous assurer que le moins de sous-réseaux ou d'hôtes nécessair es pour atteindre l'objectif d'appairage sont routables. Pour plus de détails sur l'audit de ce contrôle, consultez le document CIS Amazon Web Services Foundatio ns Benchmark version 1.4.0 disponible à l'adresse https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CIS AWS Foundations Benchmark v1.4 Level 2.

Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG1

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Center for Internet Security (CIS) Critical Security Controls v8 IG1 et les règles de AWS configuration gérées. Chacun AWS Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CIS Critical Security Controls v8 IG1. Un contrôle critique de sécurité CIS v8 IG1 peut être associé à plusieurs règles AWS Config . Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			utilisées dans votre environnement.
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-security-group-attached-to-eni	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.3	Configurer les listes de contrôle d'accès aux données	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.3	Configurer les listes de contrôle d'accès aux données	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.3	Configurer les listes de contrôle d'accès aux données	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.3	Configurer les listes de contrôle d'accès aux données	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
3.3	Configurer les listes de contrôle d'accès aux données	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.3	Configurer les listes de contrôle d'accès aux données	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3.3	Configurer les listes de contrôle d'accès aux données	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisate ur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).
3.3	Configurer les listes de contrôle d'accès aux données	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.
3.4	Appliquer la conservation des données	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Appliquer la conservation des données	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.
4.1	Établir et maintenir un processus de configuration sécurisé	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,7	Gérer les comptes par défaut sur les actifs et logiciels de l'entreprise	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.1	Établir et maintenir un inventaire des comptes	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.3	Désactiver les comptes inactifs	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Limiter les privilèges d'administrateur aux comptes d'adminis trateur dédiés	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Limiter les privilèges d'administrateur aux comptes d'adminis trateur dédiés	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparatio n des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,5	Exiger la MFA pour l'accès administratif	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Établir et maintenir un processus de gestion des journaux d'audit	audit-log-policy-exists (Vérification du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisation en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.
8.2	Collecter les journaux d'audit	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
8.2	Collecter les journaux d'audit	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
8.2	Collecter les journaux d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3	Garantir un stockage adéquat des journaux d'audit	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Déployer et maintenir un logiciel de protection contre les programmes malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2	Configurer les mises à jour automatiques des signatures contre les programmes malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).
11,3	Protéger les données de récupération	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Protéger les données de récupération	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
11,3	Protéger les données de récupération	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Protéger les données de récupération	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CIS Critical Security Controls v8 IG1.

Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG2

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Center for Internet Security (CIS) Critical Security Controls v8 IG2 et les règles de AWS configuration gérées. Chacun AWS Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CIS Critical Security Controls v8 IG2. Un contrôle critique de sécurité CIS v8 IG2 peut être associé à plusieurs règles AWS Config . Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) attribuées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux Elastic Network Interfaces (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2)

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-security-group-attached-to-eni	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2,4	Utiliser des outils d'inventaire logiciel automatisés	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2,4	Utiliser des outils d'inventaire logiciel automatisés	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.3	Configurer les listes de contrôle d'accès aux données	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.3	Configurer les listes de contrôle d'accès aux données	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.3	Configurer les listes de contrôle d'accès aux données	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.3	Configurer les listes de contrôle d'accès aux données	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
3.3	Configurer les listes de contrôle d'accès aux données	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.3	Configurer les listes de contrôle d'accès aux données	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3.3	Configurer les listes de contrôle d'accès aux données	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisate ur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).
3.3	Configurer les listes de contrôle d'accès aux données	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.
3.4	Appliquer la conservation des données	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Appliquer la conservation des données	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
3,10	Chiffrer les données sensibles en transit	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,10	Chiffrer les données sensibles en transit	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
3,10	Chiffrer les données sensibles en transit	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,10	Chiffrer les données sensibles en transit	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
3,10	Chiffrer les données sensibles en transit	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
3,11	Chiffrer les données sensibles au repos	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
3,11	Chiffrer les données sensibles au repos	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets Secrets Manager, activez le chiffrement au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
3,11	Chiffrer les données sensibles au repos	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.
4.1	Établir et maintenir un processus de configuration sécurisé	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,7	Gérer les comptes par défaut sur les actifs et logiciels de l'entreprise	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.1	Établir et maintenir un inventaire des comptes	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.3	Désactiver les comptes inactifs	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Limiter les privilèges d'administrateur aux comptes d'adminis trateur dédiés	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Limiter les privilèges d'administrateur aux comptes d'adminis trateur dédiés	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparatio n des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6	Centraliser la gestion des comptes	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,5	Exiger la MFA pour l'accès administratif	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.7	Centraliser le contrôle d'accès	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7,5	Soumettre les actifs internes de l'entreprise à des analyses de vulnérabilité automatisées	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.
8.1	Établir et maintenir un processus de gestion des journaux d'audit	audit-log-policy-exists (Vérification du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisation en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
8.2	Collecter les journaux d'audit	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
8.2	Collecter les journaux d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3	Garantir un stockage adéquat des journaux d'audit	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).
8,5	Collecter des journaux d'audit détaillés	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
8,5	Collecter des journaux d'audit détaillés	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
8,5	Collecter des journaux d'audit détaillés	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,7	Collecter des journaux d'audit des demandes d'URL	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,9	Centraliser les journaux d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
8.10	Conserver les journaux d'audit	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.10	Conserver les journaux d'audit	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Déployer et maintenir un logiciel de protection contre les programmes malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2	Configurer les mises à jour automatiques des signatures contre les programmes malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.4	Configurer l'analyse automatique des programmes malveillants sur les supports amovibles	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.6	Assurer une gestion centralisée des logiciels de protection contre les programme s malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.7	Utiliser un logiciel contre les programme s malveillants basé sur le comportement	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).
11,3	Protéger les données de récupération	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Protéger les données de récupération	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
11,3	Protéger les données de récupération	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Protéger les données de récupération	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
12.2	Établir et maintenir une architecture réseau sécurisée	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
12.2	Établir et maintenir une architecture réseau sécurisée	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
12.2	Établir et maintenir une architecture réseau sécurisée	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
12.2	Établir et maintenir une architecture réseau sécurisée	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
12.2	Établir et maintenir une architecture réseau sécurisée	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
12.2	Établir et maintenir une architecture réseau sécurisée	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
12.2	Établir et maintenir une architecture réseau sécurisée	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiquement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.
12.3	Gérer l'infrastructure réseau de manière sécurisée	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.3	Gérer l'infrastructure réseau de manière sécurisée	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
12.3	Gérer l'infrastructure réseau de manière sécurisée	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.3	Gérer l'infrastructure réseau de manière sécurisée	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
13.1	Centraliser les alertes relatives aux événements de sécurité	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13.1	Centraliser les alertes relatives aux événements de sécurité	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13,3	Déployer une solution de détection des intrusions sur le réseau	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13,6	Collecter les journaux des flux de trafic réseau	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13,6	Collecter les journaux des flux de trafic réseau	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codeb uild. Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CIS Critical Security Controls v8 IG2.

Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG3

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Center for Internet Security (CIS) Critical Security Controls v8 IG3 et les règles de AWS configuration gérées. Chacun AWS Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CIS Critical Security Controls v8 IG3. Un contrôle critique de sécurité CIS v8 IG3 peut être associé à plusieurs règles AWS Config . Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.1	Établir et tenir à jour un inventaire détaillé des actifs de l'entreprise	ec2-security-group-attached-to-eni	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Veiller à ce que les logiciels autorisés soient actuellement pris en charge	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2,4	Utiliser des outils d'inventaire logiciel automatisés	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2,4	Utiliser des outils d'inventaire logiciel automatisés	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.3	Configurer les listes de contrôle d'accès aux données	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.3	Configurer les listes de contrôle d'accès aux données	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.3	Configurer les listes de contrôle d'accès aux données	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.3	Configurer les listes de contrôle d'accès aux données	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
3.3	Configurer les listes de contrôle d'accès aux données	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.3	Configurer les listes de contrôle d'accès aux données	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.3	Configurer les listes de contrôle d'accès aux données	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3.3	Configurer les listes de contrôle d'accès aux données	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisate ur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).
3.3	Configurer les listes de contrôle d'accès aux données	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Configurer les listes de contrôle d'accès aux données	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.
3.4	Appliquer la conservation des données	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Appliquer la conservation des données	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
3,10	Chiffrer les données sensibles en transit	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,10	Chiffrer les données sensibles en transit	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
3,10	Chiffrer les données sensibles en transit	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,10	Chiffrer les données sensibles en transit	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
3,10	Chiffrer les données sensibles en transit	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,10	Chiffrer les données sensibles en transit	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
3,11	Chiffrer les données sensibles au repos	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
3,11	Chiffrer les données sensibles au repos	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets Secrets Manager, activez le chiffrement au repos pour protéger ces données.
3,11	Chiffrer les données sensibles au repos	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,11	Chiffrer les données sensibles au repos	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
3,11	Chiffrer les données sensibles au repos	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3,14	Journaliser l'accès aux données sensibles	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
3,14	Journaliser l'accès aux données sensibles	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,14	Journaliser l'accès aux données sensibles	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.
4.1	Établir et maintenir un processus de configuration sécurisé	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Établir et maintenir un processus de configuration sécurisé	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4.6	Gérer de manière sécurisée les actifs et logiciels de l'entreprise	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4,7	Gérer les comptes par défaut sur les actifs et logiciels de l'entreprise	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.1	Établir et maintenir un inventaire des comptes	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Utiliser des mots de passe uniques	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.3	Désactiver les comptes inactifs	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Limiter les privilèges d'administrateur aux comptes d'adminis trateur dédiés	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Limiter les privilèges d'administrateur aux comptes d'adminis trateur dédiés	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparatio n des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6	Centraliser la gestion des comptes	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.4	Exiger la MFA pour l'accès au réseau distant	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,5	Exiger la MFA pour l'accès administratif	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.7	Centraliser le contrôle d'accès	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1	Établir et maintenir un processus de gestion des vulnérabilités	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.3	Effectuer une gestion automatisée des correctifs du système d'exploitation	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.4	Effectuer une gestion automatisée des correctifs d'applications	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7,5	Soumettre les actifs internes de l'entreprise à des analyses de vulnérabilité automatisées	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.
8.1	Établir et maintenir un processus de gestion des journaux d'audit	audit-log-policy-exists (Vérification du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisation en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
8.2	Collecter les journaux d'audit	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
8.2	Collecter les journaux d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2	Collecter les journaux d'audit	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3	Garantir un stockage adéquat des journaux d'audit	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).
8,5	Collecter des journaux d'audit détaillés	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
8,5	Collecter des journaux d'audit détaillés	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
8,5	Collecter des journaux d'audit détaillés	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,5	Collecter des journaux d'audit détaillés	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,7	Collecter des journaux d'audit des demandes d'URL	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8,9	Centraliser les journaux d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
8.10	Conserver les journaux d'audit	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.10	Conserver les journaux d'audit	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Déployer et maintenir un logiciel de protection contre les programmes malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2	Configurer les mises à jour automatiques des signatures contre les programmes malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.4	Configurer l'analyse automatique des programmes malveillants sur les supports amovibles	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.6	Assurer une gestion centralisée des logiciels de protection contre les programmes malveillants	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.7	Utiliser un logiciel contre les programme s malveillants basé sur le comportement	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	Exécuter des sauvegardes automatiques	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).
11,3	Protéger les données de récupération	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Protéger les données de récupération	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
11,3	Protéger les données de récupération	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Protéger les données de récupération	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Établir et gérer une instance isolée de données de récupération	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
12.2	Établir et maintenir une architecture réseau sécurisée	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
12.2	Établir et maintenir une architecture réseau sécurisée	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
12.2	Établir et maintenir une architecture réseau sécurisée	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
12.2	Établir et maintenir une architecture réseau sécurisée	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
12.2	Établir et maintenir une architecture réseau sécurisée	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
12.2	Établir et maintenir une architecture réseau sécurisée	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
12.2	Établir et maintenir une architecture réseau sécurisée	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.2	Établir et maintenir une architecture réseau sécurisée	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiquement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.
12.3	Gérer l'infrastructure réseau de manière sécurisée	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.3	Gérer l'infrastructure réseau de manière sécurisée	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
12.3	Gérer l'infrastructure réseau de manière sécurisée	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.3	Gérer l'infrastructure réseau de manière sécurisée	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.3	Gérer l'infrastructure réseau de manière sécurisée	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.6	Utiliser des protocoles de communication et de gestion de réseau sécurisés	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
13.1	Centraliser les alertes relatives aux événements de sécurité	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13.1	Centraliser les alertes relatives aux événements de sécurité	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13,3	Déployer une solution de détection des intrusions sur le réseau	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13,6	Collecter les journaux des flux de trafic réseau	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13,6	Collecter les journaux des flux de trafic réseau	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13,10	Effectuer le filtrage de la couche d'applica tion	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codeb uild. Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,1	Établir et maintenir un processus de développement d'applications sécurisé	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,12	Mettre en œuvre des contrôles de sécurité au niveau du code	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,12	Mettre en œuvre des contrôles de sécurité au niveau du code	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codeb uild. Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,12	Mettre en œuvre des contrôles de sécurité au niveau du code	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.
16,12	Mettre en œuvre des contrôles de sécurité au niveau du code	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16,12	Mettre en œuvre des contrôles de sécurité au niveau du code	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CIS Critical Security Controls v8 IG3.

Bonnes pratiques de fonctionnement pour CIS Top 20

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les 20 principaux contrôles de sécurité critiques du Center for Internet Security (CIS) et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CIS Top 20. Un contrôle CIS Top 20 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Ce pack de conformité a été validé par AWS Security Assurance Services LLC (AWS SAS), qui est une équipe d'évaluateurs de sécurité qualifiés (QSA) dans le secteur des cartes de paiement, de praticiens certifiés par HITRUST Common Security Framework (CCSFP) et de professionnels de la conformité certifiés pour fournir des conseils et des évaluations pour divers frameworks industriels. AWS Les professionnels de SAS ont conçu ce pack de conformité pour permettre à un client de s'aligner sur un sous-ensemble du Top 20 de la CEI.

ID du contrôle	AWS Config Règle	Conseils
CIS.2	ec2- -check managedinstance-association-compliance-status	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
CIS.2	ec2- -check managedinstance-patch-compliance-status	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon

ID du contrôle	AWS Config Règle	Conseils
		Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politique s et procédures de votre entreprise.
CIS.2	ec2- -eni security-group-attached-to	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.
CIS.2	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant plus de jours que le nombre de jours autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.2	ec2- volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.
CIS.2	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.

ID du contrôle	AWS Config Règle	Conseils
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
CIS.3	guardduty-non-archived-find ings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classific ations pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSev (Config Default : 30), daysMediu mSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisat ion.

ID du contrôle	AWS Config Règle	Conseils
CIS.3	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Config Règle	Conseils
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
CIS.4	iam-root-access-key-vérifier	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Config Règle	Conseils
CIS.4	root-account-hardware-mfa-activé	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Config Règle	Conseils
CIS.4	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Config Règle	Conseils
CIS.4	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Config Règle	Conseils
CIS.5	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Config Règle	Conseils
CIS.5	ec2- -check managedinstance-association-compliance-status	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.
CIS.5	ec2- -check managedinstance-patch-compliance-status	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politique s et procédures de votre entreprise.

ID du contrôle	AWS Config Règle	Conseils
CIS.5	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.5	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.
CIS.6	api-gw-execution-logging-activé	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
CIS.6	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	cloud-trail-log-file-activé pour la validation	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
CIS.6	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du Compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de tous Régions AWS vers votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lance ment d'une nouvelle région, le même parcours CloudTrai l sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	s3- bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Config Règle	Conseils
CIS.6	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
CIS.6	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Config Règle	Conseils
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
CIS.9	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CIS.9	ebs-snapshot-public-restora ble-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CIS.9	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	emr-master-no-public-IP	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CIS.9	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	ec2- instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	internet-gateway-authorized-vpc-uniquement	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
CIS.9	lambda-function-public-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communica tion sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	rds-instance-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CIS.9	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CIS.9	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePub licAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPubl icAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CIS.9	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CIS.9	sagemaker-notebook-no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Config Règle	Conseils
CIS.9	vpc-default-security-group-fermé	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
CIS.9	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Config Règle	Conseils
CIS.10	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
CIS.10	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	AWS Config Règle	Conseils
CIS.10	elasticache-redis-cluster-automatic-vérification des sauvegardes	Lorsque les sauvegard es automatiques sont activées, Amazon ElastiCac he crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
CIS.10	s3- bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Config Règle	Conseils
CIS.10	s3- bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
CIS.11	ec2- -eni security-group-att ached-to	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.

ID du contrôle	AWS Config Règle	Conseils
CIS.11	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Config Règle	Conseils
CIS.11	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.11	vpc-default-security-group-fermé	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
CIS.11	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CIS.12	ebs-snapshot-public-restora ble-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CIS.12	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
CIS.12	emr-master-no-public-IP	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
CIS.12	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	ec2- instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	internet-gateway-authorized-vpc-uniquement	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
CIS.12	lambda-function-public-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communica tion sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	rds-instance-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CIS.12	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CIS.12	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePub licAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPubl icAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CIS.12	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CIS.12	sagemaker-notebook-no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
CIS.12	vpc-default-security-group-fermé	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Config Règle	Conseils
CIS.12	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
CIS.13	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.13	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
CIS.13	api-gw-cache-enabledet crypté	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
CIS.13	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
CIS.13	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Config Règle	Conseils
CIS.13	ec2- ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
CIS.13	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
CIS.13	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Config Règle	Conseils
CIS.13	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
CIS.13	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Config Règle	Conseils
CIS.13	kms-cmk-not-scheduled-pour suppression	Pour protéger les données au repos, assurez-vous que la suppression des clés principal es du client (CMK) nécessair es n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppressi on est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
CIS.13	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.13	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
CIS.13	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.13	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CIS.13	s3- bucket-default-lock-enabled	Assurez-vous que le verrouill age est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartim ents S3, appliquez le verrouill age d'objet au repos pour protéger ces données.
CIS.13	compatible avec bucket-se rver-side-encryption s3	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartim ents Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.13	s3- bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CIS.13	sagemaker-endpoint-configuration-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.13	sagemaker-notebook-instance-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
CIS.13	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
CIS.14	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CIS.14	api-gw-cache-enabledet crypté	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
CIS.14	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
CIS.14	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CIS.14	ebs-snapshot-public-restorable-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	ec2- ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
CIS.14	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
CIS.14	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Config Règle	Conseils
CIS.14	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
CIS.14	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.
CIS.14	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Config Règle	Conseils
CIS.14	kms-cmk-not-scheduled-pour suppression	Pour protéger les données au repos, assurez-vous que la suppression des clés principal es du client (CMK) nécessair es n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppressi on est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
CIS.14	rds-instance-public-access-vérifier	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
CIS.14	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CIS.14	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
CIS.14	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePub licAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPubl icAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
CIS.14	s3- bucket-default-lock-enabled	Assurez-vous que le verrouill age est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartim ents S3, appliquez le verrouill age d'objet au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	s3- bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
CIS.14	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CIS.14	compatible avec bucket-server-side-encryption s3	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
CIS.14	s3- bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	sagemaker-endpoint-configuration-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
CIS.14	sagemaker-notebook-instance-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.14	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	access-keys-rotated	Les informations d'identif ication sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organis ation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
CIS.16	guardduty-non-archived-find ings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classific ations pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSev (Config Default : 30), daysMediu mSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisat ion.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et le Centers for Internet Security (CIS) AWS Foundations Benchmark en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Config Règle	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	iam-root-access-key-vérifier	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
CIS.16	iam-user-group-membership-vérifier	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
CIS.16	iam-user-no-policies-vérifier	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	iam-user-unused-credentials-vérifier	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	mfa-enabled-for-iam-accès à la console	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	root-account-hardware-mfa-activé	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Config Règle	Conseils
CIS.16	root-account-mfa-enabled	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authent ification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisa teur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
CIS.16	secretsmanager-rotation-ena bled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiel lement réduire l'impact commercial s'il est compromis.

ID du contrôle	AWS Config Règle	Conseils
CIS.16	secretsmanager-scheduled-rotation-success-vérifier	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctem ent transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
CIS.16	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Config Règle	Conseils
CIS.18	codebuild-project-envvar-awscred-vérifier	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
CIS.18	codebuild-project-source-repo-vérification d'URL	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	AWS Config Règle	Conseils
CIS.19	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
CIS.19	guardduty-non-archived-find ings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classific ations pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSev (Config Default : 30), daysMediu mSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisat ion.

ID du contrôle	AWS Config Règle	Conseils
CIS.19	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Config Règle	Conseils
CIS.2	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CIS Top 20.

Bonnes pratiques de fonctionnement pour CISA Cyber Essentials

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les règles Cyber Essentials (CE) de la Cybersecurity & Infrastructure Security Agency (CISA) et les règles de configuration AWS gérées.

Chaque AWS Config règle s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CE CISA. Un contrôle CE CISA peut être lié à plusieurs AWS Config règles. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre personnel-1	Développez une culture de sensibilisation afin d'encourager les employés à faire des choix judicieux en ligne.	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
Votre personnel-2	Découvrez des risques tels que l'hameçonnage et la compromission des e-mails professionnels.XXXXX.	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre personnel-3	Veillez à ce que le personnel reste au fait des événement s actuels liés à la cybersécurité, en utilisant les leçons apprises et les événements signalés pour rester vigilants face à l'environ nement de menace actuel et réagir aux tendances en matière de cybersécurité.	security-awareness -program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
Votre personnel-4	Tirez parti de la formation de base en cybersécurité pour améliorer l'exposit ion aux concepts, à la terminologie et aux activités de cybersécu rité associés à la mise en œuvre des bonnes pratiques en matière de cybersécurité.	security-awareness -program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre personnel-5	Identifiez les ressources de formation disponibles par le biais d'associations professionnelles, d'établissements universitaires, du secteur privé et de sources gouvernementales.	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
Vos systèmes-1	Sachez ce qui se trouve sur votre réseau. Tenez à jour l'inventaire des actifs matériels et logiciels pour savoir ce qui est en jeu et ce qui est exposé à des risques d'attaque.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-1	Sachez ce qui se trouve sur votre réseau. Tenez à jour l'inventaire des actifs matériels et logiciels pour savoir ce qui est en jeu et ce qui est exposé à des risques d'attaque.	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-1	Sachez ce qui se trouve sur votre réseau. Tenez à jour l'inventaire des actifs matériels et logiciels pour savoir ce qui est en jeu et ce qui est exposé à des risques d'attaque.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-1	Sachez ce qui se trouve sur votre réseau. Tenez à jour l'inventaire des actifs matériels et logiciels pour savoir ce qui est en jeu et ce qui est exposé à des risques d'attaque.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-1	Sachez ce qui se trouve sur votre réseau. Tenez à jour l'inventaire des actifs matériels et logiciels pour savoir ce qui est en jeu et ce qui est exposé à des risques d'attaque.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-1	Sachez ce qui se trouve sur votre réseau. Tenez à jour l'inventaire des actifs matériels et logiciels pour savoir ce qui est en jeu et ce qui est exposé à des risques d'attaque.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-1	Sachez ce qui se trouve sur votre réseau. Tenez à jour l'inventaire des actifs matériels et logiciels pour savoir ce qui est en jeu et ce qui est exposé à des risques d'attaque.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-2	Tirez parti des mises à jour automatiques sur tous les systèmes d'exploitation et les logiciels tiers.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-2	Tirez parti des mises à jour automatiques sur tous les systèmes d'exploitation et les logiciels tiers.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-2	Tirez parti des mises à jour automatiques sur tous les systèmes d'exploitation et les logiciels tiers.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-2	Tirez parti des mises à jour automatiques sur tous les systèmes d'exploitation et les logiciels tiers.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) nécessite au moins trois nœuds de données pour garantir une haute disponibilité et une tolérance aux pannes. Le déploiement d'un domaine de OpenSearch service comportant au moins trois nœuds de données garantit les opérations du cluster en cas de défaillance d'un nœud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	secretsmanager-secret-periodic-rotation	Cette règle garantit que AWS la rotation périodique des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis. La valeur par défaut est 90 jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-3	Appliquez des configurations de sécurité pour tous les actifs matériels et logiciels.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos systèmes-4	Supprimez les actifs matériels et logiciels non pris en charge ou non autorisés des systèmes.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-1	Sachez qui se trouve sur votre réseau. Tenez à jour les inventaires des connexions réseau (utilisateurs, fournisseurs, partenaires commerciaux, etc.).	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-1	Sachez qui se trouve sur votre réseau. Tenez à jour les inventaires des connexions réseau (utilisateurs, fournisseurs, partenaires commerciaux, etc.).	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
Votre environnement-1	Sachez qui se trouve sur votre réseau. Tenez à jour les inventaires des connexions réseau (utilisateurs, fournisseurs, partenaires commerciaux, etc.).	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-2	Tirez parti d'une authentification multifactorielle appliquée à tous les utilisateurs, à commencer par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-2	Tirez parti d'une authentification multifactorielle appliquée à tous les utilisateurs, à commencer par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-2	Tirez parti d'une authentification multifactorielle appliquée à tous les utilisateurs, à commencer par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-2	Tirez parti d'une authentification multifactorielle appliquée à tous les utilisateurs, à commencer par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-3	Accordez l'accès et les autorisations d'administrateur en need-to-know fonction du moindre privilège.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-3	Accordez l'accès et les autorisations d'administrateur en need-to-know fonction du moindre privilège.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-3	Accordez l'accès et les autorisations d'administrateur en need-to-know fonction du moindre privilège.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-3	Accordez l'accès et les autorisations d'administrateur en need-to-know fonction du moindre privilège.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-3	Accordez l'accès et les autorisations d'administrateur en need-to-know fonction du moindre privilège.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-3	Accordez l'accès et les autorisations d'administrateur en need-to-know fonction du moindre privilège.	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-3	Accordez l'accès et les autorisations d'administrateur en need-to-know fonction du moindre privilège.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre environnement-4	Utilisez des mots de passe uniques pour tous les utilisateurs.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
Vos données-1	Découvrez comment vos données sont protégées.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
Vos données-1	Découvrez comment vos données sont protégées.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
Vos données-1	Découvrez comment vos données sont protégées.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
Vos données-1	Découvrez comment vos données sont protégées.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Vos données-1	Découvrez comment vos données sont protégées.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
Vos données-1	Découvrez comment vos données sont protégées.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Vos données-1	Découvrez comment vos données sont protégées.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
Vos données-1	Découvrez comment vos données sont protégées.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Vos données-1	Découvrez comment vos données sont protégées.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-1	Découvrez comment vos données sont protégées.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Vos données-1	Découvrez comment vos données sont protégées.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composants du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-v ous que le chiffreme nt est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffreme nt au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principal e propre au client (CMK).
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	rds-snapshot-encry pted	Assurez-vous que le chiffrement est activé pour vos instantan és Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-note s, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, ainsi que les activités en cours de transit data-at-rest et le comportement des utilisateurs.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composants du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composants du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composants du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-2	Découvrez ce qui se passe sur votre réseau. Gérez les composant s du réseau et du périmètre, les composants de l'hôte et du périphérique, data-at-rest ainsi que les activités en transit et le comportement des utilisateurs.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-3	Protection du système de noms de domaine.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegard es automatisées régulières des principaux systèmes.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-4	Établissez des redondances et des sauvegardes automatisées régulières des principaux systèmes.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Vos données-5	Tirez parti de protections pour les sauvegardes, parmi lesquelles la sécurité physique, le chiffrement et les copies hors ligne.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Vos données-5	Tirez parti de protections pour les sauvegardes, parmi lesquelles la sécurité physique, le chiffrement et les copies hors ligne.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre réponse à une crise-2	Dirigez le développement d'une structure de reporting interne pour détecter, communiquer et contenir les attaques.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Votre réponse à une crise-2	Dirigez le développement d'une structure de reporting interne pour détecter, communiquer et contenir les attaques.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-1	Utilisez une solution de sauvegarde qui sauvegarde automatiquement et en continu les données critiques et les configurations système.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-2	Exigez une authentification multifactorielle (MFA) pour l'accès à vos systèmes chaque fois que possible. L'authentification MFA devrait être obligatoire pour tous les utilisateurs, mais commencez par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-2	Exigez une authentification multifactorielle (MFA) pour l'accès à vos systèmes chaque fois que possible. L'authentification MFA devrait être obligatoire pour tous les utilisateurs, mais commencez par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-2	Exigez une authentification multifactorielle (MFA) pour l'accès à vos systèmes chaque fois que possible. L'authentification MFA devrait être obligatoire pour tous les utilisateurs, mais commencez par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-2	Exigez une authentification multifactorielle (MFA) pour l'accès à vos systèmes chaque fois que possible. L'authentification MFA devrait être obligatoire pour tous les utilisateurs, mais commencez par les utilisateurs privilégiés, administratifs et disposant d'un accès à distance.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-3	Activez les mises à jour automatiques dans la mesure du possible. Remplacez les systèmes d'exploitation, les applications et le matériel non pris en charge. Testez et déployez rapidement les correctifs.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-3	Activez les mises à jour automatiques dans la mesure du possible. Remplacez les systèmes d'exploitation, les applications et le matériel non pris en charge. Testez et déployez rapidement les correctifs.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-3	Activez les mises à jour automatiques dans la mesure du possible. Remplacez les systèmes d'exploitation, les applications et le matériel non pris en charge. Testez et déployez rapidement les correctifs.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
Démarrage : les premières mesures à prendre-3	Activez les mises à jour automatiques dans la mesure du possible. Remplacez les systèmes d'exploitation, les applications et le matériel non pris en charge. Testez et déployez rapidement les correctifs.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CISA Cyber Essentials.

Bonnes pratiques de fonctionnement pour la division Criminal Justice Information Services (CJIS)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les exigences de conformité des Criminal Justice Information Services (CJIS) et les règles de configuration AWS gérées. Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CJIS. Un contrôle CJIS peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.2	Formation de sensibilisation à la sécurité	security-awareness-program-exists (Vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			divers incidents ou atteintes à la sécurité.
5.3	Réponse aux incidents	response-plan-exists-maintained (Vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiellement documentés permet de s'assurer que le personnel d'intervention comprend les rôles, les responsabilités et les processus à suivre en cas d'incident.
5.3	Réponse aux incidents	response-plan-tested (Vérification du processus)	Assurez-vous que les plans de réponse et de reprise sont testés. Cela peut vous aider à comprendre si votre plan sera efficace en cas d'incident et si des lacunes doivent être corrigées ou des mises à jour effectuées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4	Vérification et responsabilisation	audit-log-policy-exists (Vérification du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisation en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.
5.4.1	Événements et contenus vérifiables (systèmes d'information)	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
5.4.1	Événements et contenus vérifiables (systèmes d'information)	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'informa tion)	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.
5.4.1	Événements et contenus vérifiables (systèmes d'information)	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
5.4.1	Événements et contenus vérifiables (systèmes d'information)	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.1	Événements et contenus vérifiables (systèmes d'information)	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
5.4.1	Événements et contenus vérifiables (systèmes d'information)	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.5	Protection des informations d'audit	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.5	Protection des informations d'audit	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.5	Protection des informations d'audit	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.
5.4.6	Conservation des enregistrements d'audit	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.4.6	Conservation des enregistrements d'audit	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
5.5.2	Exécution d'accès	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur CJIS : false), RequireLowercaseCharacters (valeur CJIS : false), (valeur CJIS : false), RequireSymbols (valeur CJIS : false), RequireNumbers (valeur CJIS : faux), MinimumPasswordLength (valeur CJIS : 8),

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			(valeur CJIS : 10) et PasswordReusePreve ntion MaxPasswo rdAge (valeur CJIS : 90) pour votre politique de mot de passe IAM. Les valeurs réelles doivent refléter les politiques de votre organisation.
5.5.2	Exécution d'accès	iam-policy-no-stat ements-with-full-a ccess	Assurez-vous que les actions IAM sont limitées aux seules actions nécessair es. Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	rds-instance-iam-authentication-enabled	Assurez-vous qu'une authentification AWS Identity and Access Management (IAM) est activée sur les instances Amazon Relational Database Service (Amazon RDS) afin de contrôler l'accès aux systèmes et aux actifs. Cela permet de chiffrer le trafic réseau à destination et en provenance de la base de données au moyen du protocole SSL. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2	Exécution d'accès	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.
5.5.2.1	Principe de moindre privilège	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
5.5.2.1	Principe de moindre privilège	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
5.5.2.1	Principe de moindre privilège	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisa teur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.2.1	Principe de moindre privilège	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.6	Accès distant	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.5.6	Accès distant	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6.2.1.1	Mot de passe	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur CJIS : false), RequireLowercaseCharacters (valeur CJIS : false), (valeur CJIS : false), RequireSymbols (valeur CJIS : false), RequireNumbers (valeur CJIS : faux), MinimumPasswordLength (valeur CJIS : 8),

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			(valeur CJIS : 10) et PasswordReusePreve ntion MaxPasswo rdAge (valeur CJIS : 90) pour votre politique de mot de passe IAM. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6.2.2	Authentification avancée	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
5.6.2.2	Authentification avancée	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6.2.2	Authentification avancée	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6.2.2	Authentification avancée	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6.2.2	Authentification avancée	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.6.3.1	Gestion des identifiants	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
5.7.1.1	Principe de moindre fonctionnalité	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
5.7.1.1	Principe de moindre fonctionnalité	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
5.7.1.1	Principe de moindre fonctionnalité	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
5.7.1.1	Principe de moindre fonctionnalité	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
5.7.1.1	Principe de moindre fonctionnalité	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.7.1.1	Principe de moindre fonctionnalité	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
5,10	Protection des systèmes et des communications et intégrité des informati ons	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informati ons	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informati ons	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informati ons	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
5,10	Protection des systèmes et des communications et intégrité des informati ons	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informations	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informations	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informations	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informations	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informations	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informations	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5,10	Protection des systèmes et des communications et intégrité des informations	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
5,10	Protection des systèmes et des communications et intégrité des informations	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
5.10.1	Exécution du flux d'informations	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
5.10.1	Exécution du flux d'informations	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
5.10.1	Exécution du flux d'informations	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
5.10.1	Exécution du flux d'informations	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
5.10.1	Exécution du flux d'informations	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
5.10.1	Exécution du flux d'informations	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
5.10.1	Exécution du flux d'informations	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
5.10.1	Exécution du flux d'informations	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1	Exécution du flux d'informations	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
5.10.1.1	Protection des limites	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
5.10.1.1	Protection des limites	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.
5.10.1.1	Protection des limites	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.1	Protection des limites	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.
5.10.1.2	Chiffrement	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
5.10.1.2	Chiffrement	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
5.10.1.2	Chiffrement	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
5.10.1.2	Chiffrement	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
5.10.1.2	Chiffrement	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
5.10.1.2	Chiffrement	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
5.10.1.2	Chiffrement	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
5.10.1.2	Chiffrement	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
5.10.1.2	Chiffrement	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
5.10.1.2	Chiffrement	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
5.10.1.2	Chiffrement	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
5.10.1.2	Chiffrement	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
5.10.1.2	Chiffrement	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
5.10.1.2	Chiffrement	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.2	Chiffrement	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.3	Outils et techniques de détection des intrusions	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.3	Outils et techniques de détection des intrusions	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.1.3	Outils et techniques de détection des intrusions	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.1	Gestion des correctifs	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.1	Gestion des correctifs	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.1	Gestion des correctifs	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.1	Gestion des correctifs	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.1	Gestion des correctifs	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.4	Alertes et conseils de sécurité	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.4	Alertes et conseils de sécurité	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5.10.4.4	Alertes et conseils de sécurité	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CJIS.

Bonnes pratiques de fonctionnement pour CMMC niveau 1

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions

correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la certification CMMC (Cybersecurity Maturity Model) de niveau 1 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CMMC de niveau 1. Un contrôle CMMC de niveau 1 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisate urs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identit é de ces utilisate urs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.211	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes d'information de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CMMC Level 1.

Bonnes pratiques de fonctionnement pour CMMC niveau 2

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la certification CMMC (Cybersecurity Maturity Model) de niveau 2 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CMMC de niveau 2. Un contrôle CMMC de niveau 2 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			La valeur réelle doit refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.2.007	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées s qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.2.159	Élaborez et mettez en œuvre des plans d'action conçus pour corriger les déficiences et réduire ou éliminer les vulnérabilités des systèmes organisationnels.	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisationnels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identit é de ces utilisate urs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.078	Exigez une complexité minimale des mots de passe et un changement de caractères lors de la création de nouveaux mots de passe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.079	Interdisez la réutilisation des mots de passe pendant un certain nombre de générations.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	response-plan-exists-maintained (Vérifica tion du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribué s au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiellement documentés permet de s'assurer que le personnel d'interve ntion comprend les rôles, les responsab ilités et les processus à suivre en cas d'incident.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
IR.2.093	Détectez et signalez les événements.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	vuln-scans-performed (Vérification du processus)	Assurez-vous que des analyses de vulnérabilité sont effectuées conformément à vos exigences de conformité. La cadence d'analyse, les outils utilisés et l'utilisation des résultats doivent être définis par votre organisation.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.211	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes d'information de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CMMC Level 2.

Bonnes pratiques de fonctionnement pour CMMC niveau 3

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou

d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la certification CMMC (Cybersecurity Maturity Model) de niveau 3 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CMMC de niveau 3. Un contrôle CMMC de niveau 3 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

> **Note**
>
> En raison des directives provisoires fournies par le DoD et l'organisme d'accréditation CMMC concernant la réciprocité FedRAMP pour les niveaux CMMC 3 à 5, il est recommandé aux clients d'utiliser les régions AWS GovCloud (États-Unis) pour le moment pour toutes les charges de travail nécessitant la conformité aux niveaux 3 à 5 de la CMMC. Par conséquent, les modèles de pack de conformité pour les niveaux 3 à 5 du programme CMMC ne sont pas disponibles dans la console du pack de conformité pour éviter toute confusion. Les clients peuvent installer indépendamment des règles de configuration qui reprennent les directives provisoires pour CMMC de niveau 3 à 5 (sans modèle de pack de conformité) CloudFormation en utilisant le fichier YAML d'exemple lié dans ce document.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisate urs et les processus autorisés en veillant à ce que les clés d'accès IAM soient

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les autres systèmes d'information).		alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.2.007	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	acm-certificate-ex piration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.051	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'enregistrements d'audit à des fins d'enquête et de réponse aux indications d'activités illégales, non autorisées, suspectes ou inhabituelles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.051	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'enregistrements d'audit à des fins d'enquête et de réponse aux indications d'activités illégales, non autorisées, suspectes ou inhabituelles.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.2.159	Élaborez et mettez en œuvre des plans d'action conçus pour corriger les déficiences et réduire ou éliminer les vulnérabilités des systèmes organisationnels.	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisationnels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identit é de ces utilisate urs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.078	Exigez une complexité minimale des mots de passe et un changement de caractères lors de la création de nouveaux mots de passe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.079	Interdisez la réutilisation des mots de passe pendant un certain nombre de générations.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.086	Désactivez les identifiants au bout d'une période d'inactiv ité définie.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.086	Désactivez les identifiants au bout d'une période d'inactivité définie.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
IR.2.093	Détectez et signalez les événements.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.187	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.187	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.190	Protégez l'authent icité des sessions de communication.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.3.190	Protégez l'authent icité des sessions de communication.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	api-gw-cache-enabl ed-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environne ment API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
SC.3.191	Protégez la confidentialité des CUI au repos.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SC.3.191	Protégez la confidentialité des CUI au repos.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC.3.191	Protégez la confident ialité des CUI au repos.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC.3.191	Protégez la confident ialité des CUI au repos.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SC.3.191	Protégez la confidentialité des CUI au repos.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
SC.3.191	Protégez la confidentialité des CUI au repos.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	opensearch-encrypt ed-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.211	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes d'information de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.213	Effectuez des analyses périodiques du système d'information et des analyses en temps réel des fichiers provenant de sources externes au fur et à mesure du téléchargement, de l'ouverture ou de l'exécution de fichiers.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur . L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CMMC Level 3.

Bonnes pratiques de fonctionnement pour CMMC niveau 4

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou

d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la certification CMMC (Cybersecurity Maturity Model) de niveau 4 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CMMC de niveau 4. Un contrôle CMMC de niveau 4 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

> **Note**
>
> En raison des directives provisoires fournies par le DoD et l'organisme d'accréditation de la CMMC concernant la réciprocité FedRAMP pour les niveaux 3 à 5 de la CMMC, il est recommandé aux clients d'utiliser les régions AWS GovCloud (États-Unis) pour le moment pour toutes les charges de travail nécessitant la conformité aux niveaux 3 à 5 de la CMMC. Par conséquent, les modèles de pack de conformité pour les niveaux 3 à 5 du programme CMMC ne sont pas disponibles dans la console du pack de conformité pour éviter toute confusion. Les clients peuvent installer indépendamment des règles de configuration qui reprennent les directives provisoires pour CMMC de niveau 3 à 5 (sans modèle de pack de conformité) CloudFormation en utilisant le fichier YAML d'exemple lié dans ce document.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les autres systèmes d'information).		alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.2.007	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	acm-certificate-ex piration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AM.4.226	Utilisez une fonctionnalité pour découvrir et identifier les systèmes dotés d'attributs de composants spécifiques (par exemple, le niveau du microprogramme, le type de système d'exploitation) dans votre inventaire.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AM.4.226	Utilisez une fonctionnalité pour découvrir et identifier les systèmes dotés d'attributs de composants spécifiques (par exemple, le niveau du microprogramme, le type de système d'exploitation) dans votre inventaire.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AM.4.226	Utilisez une fonctionnalité pour découvrir et identifier les systèmes dotés d'attributs de composants spécifiques (par exemple, le niveau du microprogramme, le type de système d'exploitation) dans votre inventaire.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.051	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'enregistrements d'audit à des fins d'enquête et de réponse aux indications d'activités illégales, non autorisées, suspectes ou inhabituelles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.051	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'enregistrements d'audit à des fins d'enquête et de réponse aux indications d'activités illégales, non autorisées, suspectes ou inhabituelles.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.054	Passez en revue les informations d'audit pour l'activité générale en plus de l'activité par machine.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.054	Passez en revue les informations d'audit pour l'activité générale en plus de l'activité par machine.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.054	Passez en revue les informations d'audit pour l'activité générale en plus de l'activité par machine.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	wafv2-logging-enab led	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identit é de ces utilisate urs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.078	Exigez une complexité minimale des mots de passe et un changement de caractères lors de la création de nouveaux mots de passe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.079	Interdisez la réutilisation des mots de passe pendant un certain nombre de générations.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.086	Désactivez les identifiants au bout d'une période d'inactiv ité définie.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.086	Désactivez les identifiants au bout d'une période d'inactivité définie.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
IR.2.093	Détectez et signalez les événements.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.150	Utilisez les renseignements sur les menaces pour aider au développement des architectures système et de sécurité, au choix des solutions de sécurité, à la surveillance, à la recherche des menaces et aux activités de réponse et de restauration.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA.4.171	Établissez et maintenez une capacité de détection des cybermena ces pour recherche r des indicateu rs de compromis sion dans les systèmes organisat ionnels et détecter, suivre et neutralis er les menaces qui échappent aux contrôles existants.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.187	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.187	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.190	Protégez l'authent icité des sessions de communication.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.3.190	Protégez l'authent icité des sessions de communication.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	api-gw-cache-enabl ed-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environne ment API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
SC.3.191	Protégez la confidentialité des CUI au repos.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SC.3.191	Protégez la confidentialité des CUI au repos.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC.3.191	Protégez la confident ialité des CUI au repos.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC.3.191	Protégez la confident ialité des CUI au repos.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SC.3.191	Protégez la confidentialité des CUI au repos.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	opensearch-encrypt ed-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.4.199	Utilisez les renseignements sur les menaces pour empêcher de manière proactive les requêtes DNS d'atteindre des domaines malveillants.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.4.199	Utilisez les renseignements sur les menaces pour empêcher de manière proactive les requêtes DNS d'atteindre des domaines malveillants.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.4.202	Utilisez des mécanismes pour analyser le code exécutable et les scripts (par exemple, sandbox) traversant les limites du réseau Internet ou d'autres limites définies par l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.211	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes d'information de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.213	Effectuez des analyses périodiques du système d'information et des analyses en temps réel des fichiers provenant de sources externes au fur et à mesure du téléchargement, de l'ouverture ou de l'exécution de fichiers.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur . L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.4.221	Utilisez les renseignements relatifs aux indicateurs de menace qui s'appliquent aux informations et systèmes devant être protégés, et recourez à des mesures d'atténuation efficaces obtenues auprès d'organisations externes pour aider à la détection des intrusions et des menaces.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CMMC Level 4.

Bonnes pratiques de fonctionnement pour CMMC niveau 5

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la certification CMMC (Cybersecurity Maturity Model) de niveau 5 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CMMC de niveau 5. Un contrôle CMMC de niveau 5 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

> **Note**
>
> En raison des directives provisoires fournies par le DoD et l'organisme d'accréditation CMMC concernant la réciprocité FedRAMP pour les niveaux CMMC 3 à 5, il est recommandé aux clients d'utiliser les régions AWS GovCloud (États-Unis) pour le moment pour toutes les charges de travail nécessitant la conformité aux niveaux 3 à 5 de la CMMC. Par conséquent, les modèles de pack de conformité pour les niveaux 3 à 5 du programme CMMC ne sont pas disponibles dans la console du pack de conformité pour éviter toute confusion. Les clients peuvent installer indépendamment des règles de configuration qui reprennent les directives provisoires pour CMMC de niveau 3 à 5 (sans modèle de pack de conformité) CloudFormation en utilisant le fichier YAML d'exemple lié dans ce document.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.001	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.002	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.1.003	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.2.007	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.007	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.008	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.013	Surveillez et contrôlez les sessions d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.2.016	Contrôlez le flux de CUI conformément aux autorisations approuvées.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	acm-certificate-ex piration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.014	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.017	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.3.018	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.4.023	Contrôlez les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.5.024	Identifiez et atténuez les risques associés aux points d'accès sans fil non identifiés connectés au réseau.	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau non utilisées peut contribuer à un inventaire et à une gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AM.4.226	Utilisez une fonctionnalité pour découvrir et identifier les systèmes dotés d'attributs de composants spécifiques (par exemple, le niveau du microprogramme, le type de système d'exploitation) dans votre inventaire.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AM.4.226	Utilisez une fonctionnalité pour découvrir et identifier les systèmes dotés d'attributs de composants spécifiques (par exemple, le niveau du microprogramme, le type de système d'exploitation) dans votre inventaire.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AM.4.226	Utilisez une fonctionnalité pour découvrir et identifier les systèmes dotés d'attributs de composants spécifiques (par exemple, le niveau du microprogramme, le type de système d'exploitation) dans votre inventaire.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.041	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.2.042	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.046	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.049	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.051	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'enregistrements d'audit à des fins d'enquête et de réponse aux indications d'activités illégales, non autorisées, suspectes ou inhabituelles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.3.051	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'enregistrements d'audit à des fins d'enquête et de réponse aux indications d'activités illégales, non autorisées, suspectes ou inhabituelles.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.053	Automatisez l'analyse des journaux d'audit pour identifier les indicateurs critiques (TTP) et/ou les activités suspectes définies par l'organisation, et prendre des mesures en conséquence.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.054	Passez en revue les informations d'audit pour l'activité générale en plus de l'activité par machine.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.054	Passez en revue les informations d'audit pour l'activité générale en plus de l'activité par machine.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.4.054	Passez en revue les informations d'audit pour l'activité générale en plus de l'activité par machine.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.5.055	Identifiez les actifs qui ne renvoient aucun rapport sur les journaux d'audit et assurez-vous que les systèmes approprié s définis par l'organis ation sont bien soumis à une journalisation.	wafv2-logging-enab led	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.3.161	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.061	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.062	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.063	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.064	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.2.065	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisationnels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.3.068	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.5.074	Vérifiez l'intégrité et l'exactitude des logiciels essentiels ou critiques en matière de sécurité tels que définis par l'organisation (par exemple, racines de confiance, vérification formelle ou signatures cryptographiques).	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.5.074	Vérifiez l'intégrité et l'exactitude des logiciels essentiels ou critiques en matière de sécurité tels que définis par l'organisation (par exemple, racines de confiance, vérification formelle ou signatures cryptographiques).	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.5.074	Vérifiez l'intégrité et l'exactitude des logiciels essentiels ou critiques en matière de sécurité tels que définis par l'organisation (par exemple, racines de confiance, vérification formelle ou signatures cryptographiques).	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.5.074	Vérifiez l'intégrité et l'exactitude des logiciels essentiels ou critiques en matière de sécurité tels que définis par l'organisation (par exemple, racines de confiance, vérification formelle ou signatures cryptographiques).	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisate urs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.076	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identit é de ces utilisate urs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.1.077	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.078	Exigez une complexité minimale des mots de passe et un changement de caractères lors de la création de nouveaux mots de passe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.079	Interdisez la réutilisation des mots de passe pendant un certain nombre de générations.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.2.081	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.083	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.086	Désactivez les identifiants au bout d'une période d'inactivité définie.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.3.086	Désactivez les identifiants au bout d'une période d'inactivité définie.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.092	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
IR.2.093	Détectez et signalez les événements.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.2.093	Détectez et signalez les événements.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.5.102	Combinez des réponses manuelles et automatisées en temps réel aux activités anormales qui correspondent à des modèles d'incidents.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.5.102	Combinez des réponses manuelles et automatisées en temps réel aux activités anormales qui correspondent à des modèles d'inciden ts.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.5.102	Combinez des réponses manuelles et automatisées en temps réel aux activités anormales qui correspondent à des modèles d'incidents.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.5.102	Combinez des réponses manuelles et automatisées en temps réel aux activités anormales qui correspondent à des modèles d'inciden ts.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.2.113	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.137	Effectuez et testez régulièrement des sauvegardes de données.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.2.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.3.139	Effectuez régulièrement des sauvegardes de données complètes, exhaustives et résilientes, tel que défini par l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RE.5.140	Assurez-vous que les installat ions de traitemen t des informations répondent aux exigences de continuit é, redondance et disponibilité de la sécurité de l'informa tion telles que définies par l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RE.5.140	Assurez-vous que les installations de traitement des informations répondent aux exigences de continuité, redondance et disponibilité de la sécurité de l'information telles que définies par l'organisation.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.2.142	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.150	Utilisez les renseignements sur les menaces pour aider au développement des architectures système et de sécurité, au choix des solutions de sécurité, à la surveillance, à la recherche des menaces et aux activités de réponse et de restauration.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RM.4.151	Effectuez des analyses pour détecter les ports non autorisés disponibles à travers les limites du réseau de périmètre , au-delà des limites du réseau Internet de l'organisation et d'autres limites définies par l'organis ation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA.4.171	Établissez et maintenez une capacité de détection des cybermena ces pour recherche r des indicateu rs de compromis sion dans les systèmes organisat ionnels et détecter, suivre et neutralis er les menaces qui échappent aux contrôles existants.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.1.175	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.2.179	Utilisez des sessions chiffrées lors de la gestion des appareils réseau.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.180	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.182	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.185	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.187	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.187	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.190	Protégez l'authent icité des sessions de communication.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.3.190	Protégez l'authent icité des sessions de communication.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.190	Protégez l'authent icité des sessions de communication.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	api-gw-cache-enabl ed-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environne ment API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-v ous que le chiffreme nt est activé pour vos Amazon CloudWatch Log Groups.
SC.3.191	Protégez la confident ialité des CUI au repos.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SC.3.191	Protégez la confident ialité des CUI au repos.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC.3.191	Protégez la confident ialité des CUI au repos.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC.3.191	Protégez la confident ialité des CUI au repos.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SC.3.191	Protégez la confidentialité des CUI au repos.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confidentialité des CUI au repos.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.3.191	Protégez la confident ialité des CUI au repos.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
SC.3.191	Protégez la confident ialité des CUI au repos.	opensearch-encrypt ed-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.4.199	Utilisez les renseignements sur les menaces pour empêcher de manière proactive les requêtes DNS d'atteindre des domaines malveillants.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.4.199	Utilisez les renseignements sur les menaces pour empêcher de manière proactive les requêtes DNS d'atteindre des domaines malveillants.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.4.202	Utilisez des mécanismes pour analyser le code exécutable et les scripts (par exemple, sandbox) traversant les limites du réseau Internet ou d'autres limites définies par l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.198	Configurez les systèmes de surveillance de manière à ce qu'ils enregistrent les paquets traversant les limites du réseau Internet de l'organisation et d'autres limites définies par l'organisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.198	Configurez les systèmes de surveillance de manière à ce qu'ils enregistrent les paquets traversant les limites du réseau Internet de l'organisation et d'autres limites définies par l'organisation.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.198	Configurez les systèmes de surveillance de manière à ce qu'ils enregistrent les paquets traversant les limites du réseau Internet de l'organisation et d'autres limites définies par l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.208	Utilisez des protections des limites adaptées et définies par l'organisation en plus des solutions disponibles dans le commerce.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.230	Veillez à la conformité des ports et des protocoles.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.5.230	Veillez à la conformité des ports et des protocoles.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.230	Veillez à la conformité des ports et des protocoles.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.5.230	Veillez à la conformité des ports et des protocoles.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.230	Veillez à la conformité des ports et des protocoles.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.230	Veillez à la conformité des ports et des protocoles.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.230	Veillez à la conformité des ports et des protocoles.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.230	Veillez à la conformité des ports et des protocoles.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.5.230	Veillez à la conformité des ports et des protocoles.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.210	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.211	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes d'information de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.1.213	Effectuez des analyses périodiques du système d'information et des analyses en temps réel des fichiers provenant de sources externes au fur et à mesure du téléchargement, de l'ouverture ou de l'exécution de fichiers.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur . L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.214	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.216	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.2.217	Identifiez les utilisations non autorisées des systèmes de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.4.221	Utilisez les renseignements relatifs aux indicateurs de menace qui s'appliquent aux informations et systèmes devant être protégés, et recourez à des mesures d'atténuation efficaces obtenues auprès d'organisations externes pour aider à la détection des intrusions et des menaces.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.222	Analysez le comportement des systèmes pour détecter et réduire l'exécution de commandes et de scripts système normaux indiquant des activités malveillantes.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.5.223	Surveillez en permanence les individus et composants systèmes afin de détecter tout comportement anormal ou suspect.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CMMC Level 5.

Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 1

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou

d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la certification du modèle de maturité de la cybersécurité (CMMC) 2.0 niveau 1 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles CMMC 2.0 de niveau 1. Un contrôle CMMC 2.0 de niveau 1 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisate urs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.1	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.1	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.1	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.2	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes d'information de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.5	Effectuez des analyses périodiques du système d'information et des analyses en temps réel des fichiers provenant de sources externes au fur et à mesure du téléchargement, de l'ouverture ou de l'exécution de fichiers.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur . L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CMMC 2.0 Level 1.

Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 2

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la certification du modèle de maturité de la cybersécurité (CMMC) 2.0 niveau 2 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles

CMMC 2.0 de niveau 2. Un contrôle CMMC 2.0 de niveau 2 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'informa tion aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés ou aux appareils (y compris les autres systèmes d'information).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.1	Limitez l'accès au système d'information aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés ou aux appareils (y compris les autres systèmes d'information).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.2	Limitez l'accès au système d'information aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L1-3.1.20	Vérifiez et contrôlez/limitez les connexions aux systèmes d'information externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
AC.L2-3.1.5	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC.L2-3.1.5	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.
AC.L2-3.1.7	Empêchez les utilisate urs non privilégi és d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et capturez l'exécution de ces fonctions dans des journaux d'audit.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC.L2-3.1.13	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessair e pour permettre la surveillance, l'analyse, l'investi gation et le signaleme nt d'activités illégales ou non autorisées du système.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.1	Créez et conservez des enregistrements et journaux d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales ou non autorisées du système.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU.L2-3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.2	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.2	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU.L2-3.3.2	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.4	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.4	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.4	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.4	Générez une alerte en cas d'échec d'un processus de journalisation d'audit.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.5	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'enregistrements d'audit à des fins d'enquête et de réponse aux indications d'activités illégales, non autorisées, suspectes ou inhabituelles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.5	Mettez en corrélati on les processus d'examen, d'analyse et de génération de rapports d'enregis trements d'audit à des fins d'enquête et de réponse aux indications d'activit és illégales, non autorisées, suspectes ou inhabituelles.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
AU.L2-3.3.8	Protégez les informati ons d'audit et les outils de journalisation d'audit contre tout accès, toute modificat ion et toute suppressi on non autorisés.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-v ous que le chiffreme nt est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU.L2-3.3.8	Protégez les informations d'audit et les outils de journalisation d'audit contre tout accès, toute modification et toute suppression non autorisés.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
CA.L2-3.12.2	Élaborez et mettez en œuvre des plans d'action conçus pour corriger les déficiences et réduire ou éliminer les vulnérabilités des systèmes organisationnels.	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.L2-3.12.3	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.L2-3.12.3	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA.L2-3.12.3	Surveillez en permanence les contrôles de sécurité pour garantir leur efficacité continue.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.2	Établissez et appliquez des paramètres de configuration de sécurité pour les produits des technologies de l'information utilisés dans les systèmes organisationnels.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisat ionnels.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.3	Suivez, examinez, approuvez ou désapprouvez et enregistrez les modifications apportées aux systèmes organisationnels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.7	Limitez, désactivez ou empêchez l'utilisation de programmes, de fonctions, de ports, de protocoles et de services non essentiels.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.9	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.9	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM.L2-3.4.9	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisate urs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.1	Identifiez les utilisateurs du système d'information, les processus agissant pour le compte des utilisateurs ou les appareils.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identit é de ces utilisate urs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L1-3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes d'information de l'organisation.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.3	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.3	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.3	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.3	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.6	Désactivez les identifiants au bout d'une période d'inactiv ité définie.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.6	Désactivez les identifiants au bout d'une période d'inactivité définie.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.7	Exigez une complexité minimale des mots de passe et un changement de caractères lors de la création de nouveaux mots de passe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.8	Interdisez la réutilisation des mots de passe pendant un certain nombre de générations.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA.L2-3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.L2-3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.L2-3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.L2-3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.L2-3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR.L2-3.6.3	Testez la capacité de réponse aux incidents de l'organisation.	response-plan-tested (Vérification du processus)	Assurez-vous que les plans de réponse et de reprise sont testés. Cela peut vous aider à comprendre si votre plan sera efficace en cas d'incident et si des lacunes doivent être corrigées ou des mises à jour effectuées.
MA.L2-3.7.5	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
MA.L2-3.7.5	Exigez une authentification multifactorielle pour établir des sessions de maintenance non locales via des connexions réseau externes et mettre fin à ces connexions une fois la maintenance non locale terminée.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA.L2-3.11.2	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA.L2-3.11.2	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA.L2-3.11.2	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA.L2-3.11.2	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant ces systèmes et applications sont identifiées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L1-3.13.1	Surveillez, contrôlez et protégez les communications de l'organisation (c'est-à-dire les informations transmises ou reçues par les systèmes d'information de l'organisation) aux limites externes et aux principales limites internes des systèmes d'information.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.4	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L2-3.13.10	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.10	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.15	Protégez l'authent icité des sessions de communication.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L2-3.13.15	Protégez l'authent icité des sessions de communication.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.15	Protégez l'authent icité des sessions de communication.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.15	Protégez l'authent icité des sessions de communication.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC.L2-3.13.15	Protégez l'authent icité des sessions de communication.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.15	Protégez l'authent icité des sessions de communication.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	api-gw-cache-enabl ed-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environne ment API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.16	Protégez la confidentialité des CUI au repos.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
SC.L2-3.13.16	Protégez la confident ialité des CUI au repos.	opensearch-encrypt ed-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.1	Identifiez, signalez et corrigez les informations et les failles du système d'information en temps opportun.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.1	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.1	Identifiez, signalez et corrigez les informati ons et les failles du système d'information en temps opportun.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.2	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes d'information de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L1-3.14.5	Effectuez des analyses périodiques du système d'information et des analyses en temps réel des fichiers provenant de sources externes au fur et à mesure du téléchargement, de l'ouverture ou de l'exécution de fichiers.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur . L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.L2-3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI.L2-3.14.7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for CMMC 2.0 Level 2.

Bonnes pratiques de fonctionnement pour les services de calcul

Ce pack de conformité contient des AWS Config règles basées sur les services de calcul. Pour plus d'informations, consultez les charges de travail de calcul. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les services informatiques.

Bonnes pratiques de fonctionnement pour la résilience des données

Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour la résilience des données.

Bonnes pratiques de fonctionnement pour les services de base de données

Ce pack de conformité contient des AWS Config règles basées sur les services de bases de données. Pour plus d'informations, voir Bases de données sur AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les services de bases de données.

Bonnes pratiques de fonctionnement pour les services de lac de données et d'analyse

Ce pack de conformité contient des AWS Config règles pour les lacs de données et les services d'analyse. Pour plus d'informations, voir Data Lakes and Analytics on AWS. Pour obtenir la liste de

toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les lacs de données et les services d'analyse.

Bonnes pratiques de fonctionnement pour DevOps

Ce pack de conformité contient des AWS Config règles basées sur l' DevOps intérieur AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for DevOps.

Bonnes pratiques de fonctionnement pour EC2

Ce pack de conformité contient des AWS Config règles basées sur EC2. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for EC2.

Bonnes pratiques de fonctionnement pour les services de chiffrement et de gestion des clés

Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour le chiffrement et la gestion des clés.

Bonnes pratiques de fonctionnement pour le guide de la cybersécurité pour les PME de l'ENISA

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de correspondance entre le guide de cybersécurité de l'Agence de l'Union européenne pour la cybersécurité (ENISA) destiné aux PME et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs guides de cybersécurité de l'ENISA pour les contrôles des PME. Un contrôle du guide de la cybersécurité pour les PME de l'ENISA peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages vers les contrôles adaptés issus du guide de la cybersécurité pour les PME de l'ENISA. Le guide de la cybersécurité pour les PME de l'ENISA est disponible ici : Guide de la cybersécurité pour les PME : 12 mesures pour sécuriser votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PUBLICATION DE POLITIQUES DE CYBERSÉCURITÉ	Des règles claires et spécifiques doivent être définies en matière de cybersécurité	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informati ons personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informati ons personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	elasticsearch-encrypted-at-rest	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon Elasticsearch Service (Amazon ES).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informati ons personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon Elasticse arch Service est activé. ode-to-no de Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informati ons personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informati ons personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées s qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informati ons personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1_DÉVELOPPEMENT D'UNE BONNE CULTURE DE LA CYBERSÉCURITÉ : PROTECTION DES DONNÉES	En vertu du règlement général sur la protection des données de l'UE, toute PME traitant ou stockant les informations personnelles appartenant à des résidents de l'UE/EEE doit s'assurer que des contrôles de sécurité appropriés sont mis en œuvre afin de protéger ces données. Cela implique de veiller à ce que tous les tiers travaillant pour le compte de la PME aient mis en place des mesures de sécurité adéquates.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2_PROPOSITION DE FORMATIONS ADÉQUATES	Offrez régulièrement des formations de sensibilisation à la cybersécurité à tous les employés afin de vous assurer qu'ils peuvent reconnaître et gérer les différent es menaces en matière de cybersécu rité. Ces formations doivent être adaptées aux PME et se concentrer sur des situations réelles. Fournissez une formation spécialis ée en cybersécu rité aux responsab les de la gestion de la cybersécurité au sein de l'entrepr ise afin de garantir qu'ils possèdent les aptitudes et les compétenc es requises pour accomplir leurs tâches.	security-awareness -program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4_ÉLABORATION D'UN PLAN DE RÉPONSE AUX INCIDENTS	Élaborez un plan de réponse aux incidents officiel contenant des directives, rôles et responsabilités clairs afin de garantir que tous les incidents de sécurité sont traités de manière rapide, professionnelle et appropriée. Dans le but de réagir rapidement aux menaces envers la sécurité, définissez les outils susceptibles d'être utilisés pour surveiller et alerter en cas d'activité suspecte ou de violation de la sécurité.	response-plan-exists-maintained (vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5_SÉCURISATION DE L'ACCÈS AUX SYSTÈMES	Encouragez chacun à utiliser une phrase secrète composée d'au moins trois mots courants aléatoire s présentant une excellente combinais on de mémorisat ion et de sécurité. Si vous optez pour un mot de passe classique, procédez comme suit : - Créez un mot de passe long comportant des lettres minuscule s et majuscules, et éventuellement des chiffres et des caractères spéciaux. - Proscrivez les termes évidents, tels que « mot de passe », les séquences de lettres ou de chiffres comme « abc » ou « 123 ». - Évitez d'utiliser des informati ons personnelles qui peuvent être trouvées en ligne. Quel que soit votre choix : - Ne réutilise	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	z pas une phrase secrète ou un mot de passe une seconde fois. - Ne partagez pas ces informations avec les collègues . - Activez l'authent ification multifact orielle. - Utilisez un gestionnaire de mots de passe dédié.		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPa sswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordR eusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5_SÉCURISATION DE L'ACCÈS AUX SYSTÈMES	Encouragez chacun à utiliser une phrase secrète composée d'au moins trois mots courants aléatoire s présentant une excellente combinais on de mémorisat ion et de sécurité. Si vous optez pour un mot de passe classique, procédez comme suit : - Créez un mot de passe long comportant des lettres minuscule s et majuscules, et éventuellement des chiffres et des caractères spéciaux. - Proscrivez les termes évidents, tels que « mot de passe », les séquences de lettres ou de chiffres comme « abc » ou « 123 ». - Évitez d'utiliser des informati ons personnelles qui peuvent être trouvées en ligne. Quel que soit votre choix : - Ne réutilise	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	z pas une phrase secrète ou un mot de passe une seconde fois. - Ne partagez pas ces informations avec les collègues . - Activez l'authent ification multifact orielle. - Utilisez un gestionnaire de mots de passe dédié.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5_SÉCURISATION DE L'ACCÈS AUX SYSTÈMES	Encouragez chacun à utiliser une phrase secrète composée d'au moins trois mots courants aléatoire s présentant une excellente combinais on de mémorisat ion et de sécurité. Si vous optez pour un mot de passe classique, procédez comme suit : - Créez un mot de passe long comportant des lettres minuscule s et majuscules, et éventuellement des chiffres et des caractères spéciaux. - Proscrivez les termes évidents, tels que « mot de passe », les séquences de lettres ou de chiffres comme « abc » ou « 123 ». - Évitez d'utiliser des informati ons personnelles qui peuvent être trouvées en ligne. Quel que soit votre choix : - Ne réutilise	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	z pas une phrase secrète ou un mot de passe une seconde fois. - Ne partagez pas ces informations avec les collègues . - Activez l'authent ification multifact orielle. - Utilisez un gestionnaire de mots de passe dédié.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5_SÉCURISATION DE L'ACCÈS AUX SYSTÈMES	Encouragez chacun à utiliser une phrase secrète composée d'au moins trois mots courants aléatoire s présentant une excellente combinais on de mémorisat ion et de sécurité. Si vous optez pour un mot de passe classique, procédez comme suit : - Créez un mot de passe long comportant des lettres minuscule s et majuscules, et éventuellement des chiffres et des caractères spéciaux. - Proscrivez les termes évidents, tels que « mot de passe », les séquences de lettres ou de chiffres comme « abc » ou « 123 ». - Évitez d'utiliser des informati ons personnelles qui peuvent être trouvées en ligne. Quel que soit votre choix : - Ne réutilise	root-account-hardw are-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	z pas une phrase secrète ou un mot de passe une seconde fois. - Ne partagez pas ces informations avec les collègues . - Activez l'authent ification multifact orielle. - Utilisez un gestionnaire de mots de passe dédié.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5_SÉCURISATION DE L'ACCÈS AUX SYSTÈMES	Encouragez chacun à utiliser une phrase secrète composée d'au moins trois mots courants aléatoire s présentant une excellente combinais on de mémorisat ion et de sécurité. Si vous optez pour un mot de passe classique, procédez comme suit : - Créez un mot de passe long comportant des lettres minuscule s et majuscules, et éventuellement des chiffres et des caractères spéciaux. - Proscrivez les termes évidents, tels que « mot de passe », les séquences de lettres ou de chiffres comme « abc » ou « 123 ». - Évitez d'utiliser des informati ons personnelles qui peuvent être trouvées en ligne. Quel que soit votre choix : - Ne réutilise	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	z pas une phrase secrète ou un mot de passe une seconde fois. - Ne partagez pas ces informations avec les collègues . - Activez l'authent ification multifact orielle. - Utilisez un gestionnaire de mots de passe dédié.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CORRECTION ET MISE À JOUR DES LOGICIELS	L'idéal est d'utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME d'effectuer les étapes suivantes : - Mettre régulièrement à jour l'ensemble des logiciels. - Activer les mises à jour automatiques dans la mesure du possible. - Identifier les logiciels et le matériel nécessitant des mises à jour manuelles. - Tenir compte des appareils mobiles et IoT.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CORRECTION ET MISE À JOUR DES LOGICIELS	L'idéal est d'utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME d'effectuer les étapes suivantes : - Mettre régulièrement à jour l'ensemble des logiciels. - Activer les mises à jour automatiques dans la mesure du possible. - Identifier les logiciels et le matériel nécessitant des mises à jour manuelles. - Tenir compte des appareils mobiles et IoT.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CORRECTION ET MISE À JOUR DES LOGICIELS	L'idéal est d'utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME d'effectuer les étapes suivantes : - Mettre régulièrement à jour l'ensemble des logiciels. - Activer les mises à jour automatiques dans la mesure du possible. - Identifier les logiciels et le matériel nécessitant des mises à jour manuelles. - Tenir compte des appareils mobiles et IoT.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CORRECTION ET MISE À JOUR DES LOGICIELS	L'idéal est d'utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME d'effectuer les étapes suivantes : - Mettre régulièrement à jour l'ensemble des logiciels. - Activer les mises à jour automatiques dans la mesure du possible. - Identifier les logiciels et le matériel nécessitant des mises à jour manuelles. - Tenir compte des appareils mobiles et IoT.	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CORRECTION ET MISE À JOUR DES LOGICIELS	L'idéal est d'utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME d'effectuer les étapes suivantes : - Mettre régulièrement à jour l'ensemble des logiciels. - Activer les mises à jour automatiques dans la mesure du possible. - Identifier les logiciels et le matériel nécessitant des mises à jour manuelles. - Tenir compte des appareils mobiles et IoT.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CORRECTION ET MISE À JOUR DES LOGICIELS	L'idéal est d'utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME d'effectuer les étapes suivantes : - Mettre régulièrement à jour l'ensemble des logiciels. - Activer les mises à jour automatiques dans la mesure du possible. - Identifier les logiciels et le matériel nécessitant des mises à jour manuelles. - Tenir compte des appareils mobiles et IoT.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CORRECTION ET MISE À JOUR DES LOGICIELS	L'idéal est d'utiliser une plateforme centralisée pour gérer les correctifs. Il est vivement recommandé aux PME d'effectuer les étapes suivantes : - Mettre régulièrement à jour l'ensemble des logiciels. - Activer les mises à jour automatiques dans la mesure du possible. - Identifier les logiciels et le matériel nécessitant des mises à jour manuelles. - Tenir compte des appareils mobiles et IoT.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	elasticsearch-encrypted-at-rest	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon Elasticsearch Service (Amazon ES).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon Elasticsearch Service est activé. ode-to-no de Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié afin de protéger les	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6_SÉCURISATION DES APPAREILS : CHIFFREMENT	Protégez les données en les chiffrant. En tant que PME, vous devez vous assurer que les données stockées sur les appareils mobiles, tels que les ordinateurs portables, les smartphones et les tablettes, sont chiffrées. Pour les données transférées via des réseaux publics, tels que les réseaux d'hôtels ou d'aéroports, assurez-vous que WiFi les données sont cryptées, soit en utilisant un réseau privé virtuel (VPN), soit en accédant à des sites Web via des connexions sécurisées à l'aide du protocole SSL/TLS. Veillez à utiliser pour votre propre site Web une technologie de chiffrement approprié e afin de protéger les	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	données des clients circulant sur Internet.		
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	netfw-policy-rule-group-associated	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic, et vous définissez la gestion du trafic par défaut.
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans condition s peut entraîner un comportement involontaire.
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : UTILISATION DE PARE-FEUX	Les pare-feux gèrent le trafic entrant et sortant d'un réseau et constituent un outil essentiel dans la protection des systèmes des PME. Des pare-feux doivent être déployés en vue de protéger tous les systèmes critiques, en particulier le réseau des PME face aux menaces sur Internet.	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL Web est vide, le trafic Web n'est pas détecté ni traité par le WAF.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulière ment revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particuli er vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographi ques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessair es pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulière ment revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particuli er vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographi ques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessair es pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés dans les domaines du service Amazon Elasticsearch et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulière ment revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particuli er vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographi ques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessair es pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulière ment revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particuli er vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographi ques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessair es pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulière ment revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particuli er vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographi ques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessair es pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulièrement revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particulier vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographiques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessaires pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7_SÉCURISATION DU RÉSEAU : ANALYSE DES SOLUTIONS D'ACCÈS À DISTANCE	En tant que PME, vous devez régulière ment revoir tous les outils d'accès à distance afin de vous assurer qu'ils sont sécurisés, en particuli er vous devez : - veiller à ce que tous les logiciels d'accès à distance soient corrigés et à jour ; - bloquer l'accès à distance dans les zones géographi ques suspectes ou de certaines adresses IP ; - restreindre l'accès à distance du personnel aux seuls systèmes et ordinateurs nécessair es pour travailler ; - générer des mots de passe forts pour les accès à distance et, dans la mesure du possible, activer l'authentification multifactorielle ; - vérifier que les fonctionnalités de surveillance et d'alerte	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référenti els de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionn alités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sont activées dans le but d'avertir en cas de soupçons d'attaques ou d'activités inhabituelles.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	aurora-resources-p rotected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	backup-plan-min-fr equency-and-min-re tention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegard e est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e. Cette règle vous permet de définir les paramètres requiredFrequencyV alue (Config par défaut : 1), requiredR etentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressource s qui empêche la suppression de points de restaurat ion. L'utilisation d'une politique basée sur les ressource s pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e. Cette règle vous permet de définir le paramètre requiredR etentionDays (par défaut de configura tion : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	ec2-resources-prot ected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	fsx-resources-prot ected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	rds-resources-prot ected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	redshift-backup-en abled	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos clusters Amazon Redshift disposent d'instant anés automatisés. Lorsque les instantan és automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modificat ion des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9_SÉCURISATION DES SAUVEGARDES	La gestion efficace des sauvegard es constitue une stratégie de reprise après sinistre adaptée, par exemple, suite à une attaque de rançongiciel, et permet de reprendre la génération de clés. Les règles de sauvegarde suivantes doivent s'appliqu er : - Effectuer des sauvegardes de façon régulière et automatis ée dans la mesure du possible. - Conserver les sauvegardes séparément de l'environnement de production de la PME. - Chiffrer les sauvegardes, en particulier si elles sont déplacées d'un site à un autre. - Tester la capacité à restaurer régulière ment les données à partir des sauvegard es. Idéalement, le processus de	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	restauration complète du début à la fin doit faire l'objet de tests réguliers.		
11_SÉCURISATION DU SITE EN LIGNE	En tant que PME, il est essentiel de vous assurer que votre site Web en ligne est configuré et géré de manière sécurisée et que toutes les données personnel les ou financières, telles que les données de carte de crédit, sont protégées de manière approprié e. Cela implique de réaliser régulièrement des tests de sécurité afin d'identifier les faiblesses potentiel les du site Web en matière de sécurité et de procéder à des contrôles réguliers pour s'assurer que le site est correctement géré et mis à jour.	vuln-management-pl an-exists (vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiell ement définis pour remédier aux vulnérabilités dans votre environnement.

Modèle

Le modèle est disponible sur GitHub : Guide des meilleures pratiques opérationnelles pour la cybersécurité de l'ENISA destiné aux PME.

Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau faible)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les contrôles du framework Spain Esquema Nacional de Seguridad (ENS) Low et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une ressource AWS spécifique et concerne un ou plusieurs contrôles de niveau faible prévus par l'ENS Espagne. Un contrôle de l'ENS Espagne peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages avec des contrôles de niveau faible au sein du cadre de l'ENS Espagne, dont la dernière mise à jour a eu lieu le 23/10/2020.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une

ID du contrôle	AWS Règle de configuration	Conseils
		clé principale propre au client (CMK).
Annexe II 4.1.2.a) b) c)	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.
Annexe II 4.1.2.a) b) c)	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 4.1.2.a) b) c)	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Annexe II 4.1.2.a) b) c)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
Annexe II 4.1.2.a) b) c)	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
Annexe II 4.1.2.a) b) c)	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Annexe II 4.1.2.a) b) c)	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 4.1.2.a) b) c)	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 4.1.2.a) b) c)	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Annexe II 4.1.2.a) b) c)	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.
Annexe II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
Annexe II 4.1.2.b)	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.
Annexe II 4.1.2.b)	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.1.a)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Annexe II 4.2.1.a) b)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.4	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
Annexe II 4.2.4	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Annexe II 4.2.4	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_po licy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5 FAIBLE a)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5 FAIBLE c)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 4.2.6 FAIBLE c)	elasticsearch-logs-to-cloud watch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe II 4.2.6 FAIBLE c)	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Annexe II 4.2.6 FAIBLE c)	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe II 4.2.6 FAIBLE c)	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Annexe II 4.2.6 FAIBLE c)	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Annexe II 4.2.6 FAIBLE c)	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7 FAIBLE	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
Annexe II 4.2.7 FAIBLE	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7 FAIBLE	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7 FAIBLE	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
Annexe II 4.3.1	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.
Annexe II 4.3.1	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
Annexe II 4.3.2.b)	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe II 4.3.2.b)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
Annexe II 4.3.2.b)	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involonta ire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
Annexe II 4.3.2.b)	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe II 4.3.2.b)	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Annexe II 4.3.2.b)	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
Annexe II 4.3.2.b)	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Annexe II 4.3.2.b)	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Annexe II 4.3.2.b)	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
Annexe II 4.3.2.b)	s3-bucket-public-read-prohi bited	Gérez l'accès aux ressource s dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartim ents Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classific ation des données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Annexe II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
Annexe II 4.3.2.b)	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
Annexe II 4.3.4 c)	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe II 4.3.8 FAIBLE	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Annexe II 4.3.8 FAIBLE	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe II 4.3.8 FAIBLE	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Annexe II 4.3.8 FAIBLE	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Annexe II 4.3.8 FAIBLE	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.10.b)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
Annexe II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégri té des CloudTrail journaux. La validation du fichier journal permet de détermine r si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison . Cette fonctionnalité est créée grâce à des algorithm es standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.10.d)	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
Annexe II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.6.2 BASIQUE	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
Annexe II 5.2.3	security-awareness-program-exists (Vérification du processus)	Élaborez et maintenez un programme de sensibili sation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3 FAIBLE a)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 5.6.1.c)	codebuild-project-envvar-aw scred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_ KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
Annexe II 5.6.1.c)	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
Annexe II 5.7.3	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.7.3	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.7.3	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.3	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 5.7.3	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Annexe II 5.7.3	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
Annexe II 5.7.3	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
Annexe II 5.7.3	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
Annexe II 5.7.3	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.7.3	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Annexe II 5.7.3	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 5.7.3	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
Annexe II 5.7.3	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.3	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.4	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.4	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
Annexe II 5.8.2	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.2	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Article 14.4	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
Article 16	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
Article 16	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Article 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Article 16	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_po licy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	AWS Règle de configuration	Conseils
Article 20.2	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.
Article 20.2	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politique s et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
Article 20.2	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
Article 20.2	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
Article 21.1	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Article 21.1	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibi lité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Article 21.1	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Article 21.1	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	s3-bucket-default-lock-enabled	Assurez-vous que le verrouill age est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartim ents S3, appliquez le verrouill age d'objet au repos pour protéger ces données.
Article 21.1	s3-default-encryption-kms	Assurez-vous que le chiffreme nt est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartim ent Amazon S3, activez le chiffrement au repos pour protéger ces données.
Article 21.1	sagemaker-notebook-instance -kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Article 21.1	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Article 21.1	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Article 21.1	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
Article 21.1	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
Article 21.1	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Article 21.1	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Article 21.1	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Article 21.1	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Article 21.1	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
Article 21.1	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Article 21.1	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Article 21.1	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Article 21.1	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffreme nt au repos pour protéger ces données.
Article 21.1	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponi ble. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indispo nibilité de votre passerelle client, vous pouvez configure r une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
Article 22	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
Article 22	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Article 22	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
Article 22	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Article 22	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
Article 22	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Article 22	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Article 22	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
Article 22	s3-bucket-public-read-prohi bited	Gérez l'accès aux ressource s dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartim ents Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classific ation des données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Article 22	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
Article 22	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
Article 23	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Article 23	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Article 23	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Article 23	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Article 23	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Article 23	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
Article 25	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
Article 25	db-instance-backup-enabled	La fonctionnalité de sauvegard e d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.
Article 25	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémen taire dédiée aux opération s d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opération s d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
Article 25	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low.

Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau modéré)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les contrôles du framework Spain Esquema Nacional de Seguridad (ENS) Medium et les règles de AWS configuration gérées. Chaque

règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles Spain ENS Medium. Un contrôle de l'ENS Espagne peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages avec des contrôles de niveau modéré au sein du cadre de l'ENS Espagne, dont la dernière mise à jour a eu lieu le 23/10/2020.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
Annexe II 4.1.2.a) b) c)	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node

ID du contrôle	AWS Règle de configuration	Conseils
		Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 4.1.2.a) b) c)	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Annexe II 4.1.2.a) b) c)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
Annexe II 4.1.2.a) b) c)	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
Annexe II 4.1.2.a) b) c)	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Annexe II 4.1.2.a) b) c)	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 4.1.2.a) b) c)	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 4.1.2.a) b) c)	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Annexe II 4.1.2.a) b) c)	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.
Annexe II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
Annexe II 4.1.2.b)	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.
Annexe II 4.1.2.b)	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.1.a)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Annexe II 4.2.1.a) b)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.4	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
Annexe II 4.2.4	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Annexe II 4.2.4	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_po licy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5.a)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5.c)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 4.2.6 FAIBLE c)	opensearch-logs-to-cloudwat ch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6.c)	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6.c)	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe II 4.2.6.c)	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6.c)	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Annexe II 4.2.6.c)	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6.c)	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Annexe II 4.2.6.c)	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6.c)	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Annexe II 4.2.6.c)	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
Annexe II 4.2.7	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
Annexe II 4.3.1	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
Annexe II 4.3.1	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.
Annexe II 4.3.1	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
Annexe II 4.3.2.b)	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe II 4.3.2.b)	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
Annexe II 4.3.2.b)	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe II 4.3.2.b)	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe II 4.3.2.b)	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe II 4.3.2.b)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
Annexe II 4.3.2.b)	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Annexe II 4.3.2.b)	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Annexe II 4.3.2.b)	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
Annexe II 4.3.2.b)	s3-bucket-public-read-prohi bited	Gérez l'accès aux ressource s dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartim ents Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classific ation des données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Annexe II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
Annexe II 4.3.2.b)	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
Annexe II 4.3.4 c)	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
Annexe II 4.3.7.a)	response-plan-exists-mainta ined (Vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribué s au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiell ement documentés permet de s'assurer que le personnel d'intervention comprend les rôles, les responsabilités et les processus à suivre en cas d'incident.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe II 4.3.8	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Annexe II 4.3.8	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe II 4.3.8	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Annexe II 4.3.8	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Annexe II 4.3.8	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
Annexe II 4.3.8 MODÉRÉ	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
Annexe II 4.3.10.b)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
Annexe II 4.3.10.d)	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
Annexe II 4.6.2	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
Annexe II 5.2.3	security-awareness-program-exists (Vérification du processus)	Élaborez et maintenez un programme de sensibili sation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.4.2	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.4.2	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 5.4.2	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.4.2	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.4.2	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2 MODÉRÉ	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
Annexe II 5.4.3	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.4.3	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.4.3	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Annexe II 5.4.3	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.4.3	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.4.3 MODÉRÉ	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3.a)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 5.6.1.c)	codebuild-project-envvar-aw scred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_ KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
Annexe II 5.6.1.c)	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
Annexe II 5.7.3	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.7.3	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.7.3	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.3	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 5.7.3	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Annexe II 5.7.3	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
Annexe II 5.7.3	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
Annexe II 5.7.3	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
Annexe II 5.7.3	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.7.3	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Annexe II 5.7.3	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 5.7.3	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
Annexe II 5.7.3	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.3	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.4	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.4	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que les clés principales du client (CMK) nécessaires ne sont pas programmées pour être supprimées dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
Annexe II 5.8.2	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.2	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe II 5.8.3.b)	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3.b)	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe II 5.8.3.b)	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3.b)	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 5.8.3.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3.b)	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3.b)	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3.b)	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Article 14.4	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Article 16	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
Article 16	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Article 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Article 16	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
Article 20.2	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
Article 20.2	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
Article 20.2	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
Article 20.2	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabi lités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.
Article 21.1	dynamodb-table-encrypted-km s	Assurez-vous que le chiffreme nt est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffreme nt au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
Article 21.1	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.
Article 21.1	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Article 21.1	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Article 21.1	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Article 21.1	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Article 21.1	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Article 21.1	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Article 21.1	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
Article 21.1	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
Article 21.1	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Article 21.1	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Article 21.1	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Article 21.1	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Article 21.1	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
Article 21.1	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Article 21.1	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Article 21.1	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Article 21.1	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
Article 21.1	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
Article 22	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
Article 22	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Article 22	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Article 22	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
Article 22	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirecti onnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Article 22	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Article 22	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
Article 22	s3-bucket-public-read-prohi bited	Gérez l'accès aux ressource s dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartim ents Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classific ation des données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Article 22	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
Article 22	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
Article 23	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Article 23	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Article 23	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Article 23	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Article 23	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Article 23	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Article 24.1	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
Article 24.2	response-plan-exists-mainta ined (Vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribué s au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiell ement documentés permet de s'assurer que le personnel d'intervention comprend les rôles, les responsabilités et les processus à suivre en cas d'incident.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
Article 25	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
Article 25	db-instance-backup-enabled	La fonctionnalité de sauvegard e d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.
Article 25	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémen taire dédiée aux opération s d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opération s d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
Article 25	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour Esquema Nacional de Seguridad (ENS) Medium.

Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau élevé)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les contrôles du framework Spain Esquema Nacional de Seguridad (ENS) High et les règles de AWS configuration gérées. Chaque

règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles Spain ENS High. Un contrôle de l'ENS Espagne peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages avec des contrôles de niveau élevé au sein du cadre de l'ENS Espagne, dont la dernière mise à jour a eu lieu le 09/07/2021.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.1 ÉLEVÉ	annual-risk-assessment-performed (Vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisat ion. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.
4.2.1.b)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
4.2.5. ÉLEVÉ a)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés

ID du contrôle	AWS Règle de configuration	Conseils
		d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Annexe II 4.1.2.a) b) c)	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
Annexe II 4.1.2.a) b) c)	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibi lité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 4.1.2.a) b) c)	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Annexe II 4.1.2.a) b) c)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
Annexe II 4.1.2.a) b) c)	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
Annexe II 4.1.2.a) b) c)	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Annexe II 4.1.2.a) b) c)	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 4.1.2.a) b) c)	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 4.1.2.a) b) c)	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Annexe II 4.1.2.a) b) c)	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 4.1.2.a) b) c)	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.a) b) c)	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 4.1.2.a) b) c)	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponi ble. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indispo nibilité de votre passerelle client, vous pouvez configure r une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.
Annexe II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
Annexe II 4.1.2.b)	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.1.2.b)	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.
Annexe II 4.1.2.b)	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.1.a)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Annexe II 4.2.4	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.4	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Annexe II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.4	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
Annexe II 4.2.5	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5 FAIBLE a)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.5 FAIBLE c)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 4.2.6 ÉLEVÉ b)	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifact orielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 ÉLEVÉ b)	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 ÉLEVÉ b)	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 ÉLEVÉ b)	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
Annexe II 4.2.6 FAIBLE c)	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe II 4.2.6 FAIBLE c)	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Annexe II 4.2.6 FAIBLE c)	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe II 4.2.6 FAIBLE c)	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Annexe II 4.2.6 FAIBLE c)	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.6 FAIBLE c)	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Annexe II 4.2.6 FAIBLE c)	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7 FAIBLE	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
Annexe II 4.2.7 FAIBLE	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7 FAIBLE	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.2.7 FAIBLE	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
Annexe II 4.3.1	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
Annexe II 4.3.1	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.
Annexe II 4.3.1	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveille r les EIP non utilisées dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.1	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
Annexe II 4.3.2.b)	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe II 4.3.2.b)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 4.3.2.b)	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe II 4.3.2.b)	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe II 4.3.2.b)	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Annexe II 4.3.2.b)	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
Annexe II 4.3.2.b)	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Annexe II 4.3.2.b)	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Annexe II 4.3.2.b)	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Annexe II 4.3.2.b)	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Annexe II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
Annexe II 4.3.2.b)	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
Annexe II 4.3.4 c)	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
Annexe II 4.3.7 MODÉRÉ a)	response-plan-exists-mainta ined (Vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribué s au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiell ement documentés permet de s'assurer que le personnel d'intervention comprend les rôles, les responsabilités et les processus à suivre en cas d'incident.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe II 4.3.8 FAIBLE	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Annexe II 4.3.8 FAIBLE	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe II 4.3.8 FAIBLE	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Annexe II 4.3.8 FAIBLE	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 FAIBLE	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Annexe II 4.3.8 FAIBLE	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 MODÉRÉ	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 MODÉRÉ	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 MODÉRÉ	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe II 4.3.8 MODÉRÉ	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 MODÉRÉ	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Annexe II 4.3.8 MODÉRÉ	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe II 4.3.8 MODÉRÉ	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 MODÉRÉ	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Annexe II 4.3.8 MODÉRÉ	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 MODÉRÉ	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.8 MODÉRÉ	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Annexe II 4.3.8 MODÉRÉ	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.10.b)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
Annexe II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégri té des CloudTrail journaux. La validation du fichier journal permet de détermine r si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison . Cette fonctionnalité est créée grâce à des algorithm es standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.3.10.d)	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
Annexe II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.6.2 ÉLEVÉ	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 4.6.2 BASIQUE	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
Annexe II 4.6.2 MODÉRÉ	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.2.3	security-awareness-program-exists (Vérification du processus)	Élaborez et maintenez un programme de sensibili sation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
Annexe II 5.2.4	security-awareness-program-exists (Vérification du processus)	Élaborez et maintenez un programme de sensibili sation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
Annexe II 5.2.5	security-awareness-program-exists (Vérification du processus)	Élaborez et maintenez un programme de sensibili sation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2 MODÉRÉ	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.4.2 MODÉRÉ	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2 MODÉRÉ	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.4.2 MODÉRÉ	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 5.4.2 MODÉRÉ	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2 MODÉRÉ	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.4.2 MODÉRÉ	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
Annexe II 5.4.2 MODÉRÉ	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.2 MODÉRÉ	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3 FAIBLE a)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 5.4.3 MODÉRÉ	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.4.3 MODÉRÉ	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3 MODÉRÉ	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.4.3 MODÉRÉ	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 5.4.3 MODÉRÉ	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3 MODÉRÉ	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.4.3 MODÉRÉ	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
Annexe II 5.4.3 MODÉRÉ	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.4.3 MODÉRÉ	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.6.1.c)	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.6.1.c)	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
Annexe II 5.7.3	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 5.7.3	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe II 5.7.3	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.3	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.3	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Annexe II 5.7.3	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Annexe II 5.7.3	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
Annexe II 5.7.3	cloudwatch-log-group-encryp ted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
Annexe II 5.7.3	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
Annexe II 5.7.3	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe II 5.7.3	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Annexe II 5.7.3	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe II 5.7.3	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe II 5.7.3	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
Annexe II 5.7.3	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.3	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
Annexe II 5.7.4	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.7.4	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
Annexe II 5.8.2	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.2	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe II 5.8.3 MODÉRÉ b)	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3 MODÉRÉ b)	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe II 5.8.3 MODÉRÉ b)	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3 MODÉRÉ b)	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Annexe II 5.8.3 MODÉRÉ b)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3 MODÉRÉ b)	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3 MODÉRÉ b)	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe II 5.8.3 MODÉRÉ b)	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Article 14.4	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Article 16	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
Article 16	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Article 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Article 16	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
Article 20.2	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
Article 20.2	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
Article 20.2	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
Article 20.2	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabi lités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.
Article 21.1	dynamodb-table-encrypted-km s	Assurez-vous que le chiffreme nt est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffreme nt au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
Article 21.1	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.
Article 21.1	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Article 21.1	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Article 21.1	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Article 21.1	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Article 21.1	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
Article 21.1	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configuré es avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
Article 21.1	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
Article 21.1	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
Article 21.1	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Article 21.1	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Article 21.1	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
Article 21.1	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
Article 21.1	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
Article 21.1	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Article 21.1	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Article 21.1	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Article 21.1	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 21.1	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
Article 21.1	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
Article 22	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
Article 22	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Article 22	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Article 22	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Article 22	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
Article 22	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communica tion sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
Article 22	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Article 22	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.
Article 22	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Article 22	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Article 22	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
Article 22	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Article 22	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
Article 23	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Article 23	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
Article 23	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Article 23	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
Article 23	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
Article 23	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
Article 23	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
Article 24.2	response-plan-exists-maintained (Vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiellement documentés permet de s'assurer que le personnel d'intervention comprend les rôles, les responsabilités et les processus à suivre en cas d'incident.
Article 24.1	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
Article 25	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
Article 25	db-instance-backup-enabled	La fonctionnalité de sauvegard e d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.
Article 25	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémen taire dédiée aux opération s d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opération s d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
Article 25	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
Article 25	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour Esquema Nacional de Seguridad (ENS) High.

Bonnes pratiques de fonctionnement pour la norme FDA CFR Titre 21 Partie 11

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le titre 21 du Code of Federal Regulations (CFR) Part 11 et les règles de configuration AWS gérées. Chaque AWS Config règle s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles du titre 21 du CFR Part 11 de la FDA. Un contrôle de la norme FDA CFR Titre 21 Partie 11 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :		ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	ebs-optimized-inst ance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	redshift-backup-en abled	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos clusters Amazon Redshift disposent d'instant anés automatisés. Lorsque les instantan és automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modificat ion des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.1	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants :	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	backup-plan-min-fr equency-and-min-re tention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegard e est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e. Cette règle vous permet de définir les paramètres requiredFrequencyV alue (Config par défaut : 1), requiredR etentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressource s qui empêche la suppression de points de restaurat ion. L'utilisation d'une politique basée sur les ressource s pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactitude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisa tion des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrai l, en vérifiant l'activat ion de plusieurs paramètres. Il s'agit notamment de l'utilisa tion du chiffreme nt des journaux, de la validation des journaux et de AWS CloudTrail l'activat ion dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ebs-optimized-inst ance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ec2-resources-prot ected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	redshift-backup-en abled	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos clusters Amazon Redshift disposent d'instant anés automatisés. Lorsque les instantan és automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modificat ion des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (a)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (a) Valider les systèmes afin d'assurer l'exactit ude, la fiabilité, la cohérence des performances prévues et le repérage des enregistrements modifiés ou non valides.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	cw-loggroup-retent ion-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisant e pour faciliter le dépannage et les enquêtes judiciair es. Le manque de données disponibl es dans les journaux d'événements passés complique la reconstit ution et l'identification des événement s potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	ecr-private-lifecycle-policy-configured	Les politiques de cycle de vie Amazon Elastic Container Repository (ECR) vous permettent de préciser la gestion du cycle de vie des images dans un référentiel. Cela permet l'automat isation du nettoyage des images inutilisé es en faisant, par exemple, expirer des images selon leur âge ou leur décompte.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantanée tout au long de leur période de conservation.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	s3-bucket-public-w rite-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	sagemaker-endpoint -configuration-kms- key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	sagemaker-notebook -instance-kms-key- configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-note s, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (c)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (c) Protéger les enregistrements dans le but de les récupérer de manière précise et instantan ée tout au long de leur période de conservat ion.	sagemaker-notebook -no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisate urs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourci r la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	account-part-of-or ganizations	La gestion centralis ée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernan ce centralisée des comptes peut entraîner des configura tions de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	dynamodb-table-enc rypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffreme nt au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principal e propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ec2-instance-no-pu blic-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informati ons administratives sur chaque principal.
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-policy-no-stat ements-with-full-a ccess	Assurez-vous que les actions IAM sont limitées aux seules actions nécessair es. Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	root-account-hardw are-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	s3-account-level-p ublic-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePub licAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuck ets les paramètre s (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	s3-bucket-level-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	s3-bucket-public-w rite-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	sagemaker-notebook -no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	secretsmanager-rot ation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiel lement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	secretsmanager-sch eduled-rotation-su ccess-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformém ent au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiel lement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	ssm-document-not-p ublic	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (d)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (d) Limiter l'accès au système uniquement aux personnes autorisées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisate urs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourci r la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	cw-loggroup-retent ion-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisant e pour faciliter le dépannage et les enquêtes judiciair es. Le manque de données disponibl es dans les journaux d'événements passés complique la reconstit ution et l'identification des événement s potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalente ou plus longue que celle exigée pour les dossiers électroniques concernés et doit rester disponible pour examen et être copiée par l'organisme.		que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalente ou plus longue que celle exigée pour les dossiers électroniques concernés et doit rester disponible pour examen et être copiée par l'organisme.		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépendante la date et l'heure des entrées et des actions des opérateurs qui créent, modifient ou suppriment des enregistrements	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisate urs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (e)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (e) Utiliser des pistes d'audit sécurisées, générées par ordinateur et horodatées pour enregistrer de manière indépenda nte la date et l'heure des entrées et des actions des opérateur s qui créent, modifient ou suppriment des enregistrements	wafv2-logging-enab led	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	électroniques. Le fait d'enregistrer les modifications ne doit pas masquer les information précédemment enregistrées. Toute la documentation des pistes d'audit doit être conservée pendant une période équivalen te ou plus longue que celle exigée pour les dossiers électroni ques concernés et doit rester disponible pour examen et être copiée par l'organis me.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisate urs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourci r la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	account-part-of-or ganizations	La gestion centralis ée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernan ce centralisée des comptes peut entraîner des configura tions de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	dynamodb-table-enc rypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffreme nt au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principal e propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ec2-instance-no-pu blic-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opérati on en cours.		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPa sswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordR eusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, ainsi que la non-répudiation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroniquement un enregistrement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-policy-no-stat ements-with-full-a ccess	Assurez-vous que les actions IAM sont limitées aux seules actions nécessair es. Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-user-group-mem bership-check	AWS Identity and Access Managemen t (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisate urs plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	iam-user-unused-cr edentials-check	AWS Identity and Access Managemen t (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCreden tialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		Lambda doivent être attribuées à un VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référenti els de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionn alités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	root-account-hardw are-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	s3-account-level-p ublic-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePub licAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuck ets les paramètre s (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	s3-bucket-level-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	s3-bucket-public-w rite-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	secretsmanager-rot ation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiel lement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	secretsmanager-sch eduled-rotation-su ccess-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformém ent au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiel lement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (g)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (g) Mettre en œuvre des contrôles d'autorisation afin de garantir que seules les personnes autorisées peuvent utiliser le système, signer électroni quement un enregistr ement, accéder à une opération ou à l'appareil d'entrée ou de sortie du système	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informatique, modifier un enregistrement ou mener à bien l'opération en cours.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (h)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants : (h) Utilisati on de contrôles de l'appareil (par exemple, un terminal) pour déterminer, le cas échéant, la validité de la source de saisie des données ou des instructions opérationnelles.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (h)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants : (h) Utilisati on de contrôles de l'appareil (par exemple, un terminal) pour déterminer, le cas échéant, la validité de la source de saisie des données ou des instructions opérationnelles.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (h)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure les éléments suivants : (h) Utilisati on de contrôles de l'appareil (par exemple, un terminal) pour déterminer, le cas échéant, la validité de la source de saisie des données ou des instructions opérationnelles.	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (i)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (i) Détermine r si les personnes qui développent, conservent ou utilisent des systèmes d'enregistrement/d e signature électroni que possèdent les connaissances, les compétences et l'expérience nécessair es pour accomplir les	security-awareness -program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tâches qui leur sont confiées.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	autoscaling-launch -config-public-ip- disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	s3-account-level-p ublic-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePub licAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuck ets les paramètre s (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	s3-bucket-public-w rite-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	ssm-document-not-p ublic	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.10 (k)	Les utilisateurs de systèmes fermés qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, ainsi que la non-répud iation de ces derniers. Ces procédures et contrôles doivent inclure l'élément suivant : (k) Mettre en place des contrôles appropriés sur la documentation des systèmes, y compris (1) des contrôles adéquats sur la distribution, l'accès et l'utilisation de la documentation pour le fonctionn ement et la maintenan ce du système ;	s3-bucket-level-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	(2) des procédures de contrôle des modifications et de révision en vue de conserver une piste d'audit contenant les informations relatives à la création et à la modification séquencées dans le temps de la documentation des systèmes.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	(a) Les utilisateurs de signatures électroniques non basées sur la biométrie doivent : (1) recourir à au moins deux méthodes d'identification distinctes, telles qu'un code d'identification et un mot de passe. (i) Lorsqu'une personne exécute une série de signatures lors d'un seul accès continu et contrôlé au système, elle doit apposer la première signature en utilisant tous les composants relatifs à la signature électronique ; les signatures suivantes doivent être apposées à l'aide d'au moins un composant de signature électronique qui ne peut être exécuté que par son propriétaire et généré exclusivement pour celui-ci. (ii) Lorsqu'une personne exécute une ou plusieurs	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	signatures électroniques en dehors d'un seul accès continu et contrôlé au système, elle doit apposer chacune des signatures en utilisant tous les composants relatifs à la signature électronique ; (2) utiliser la signature électronique dont ils sont légitimement propriétaires ; (3) gérer et exécuter les signatures électroniques de manière à garantir que toute tentative d'utilisation d'une signature électronique par un individu autre que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	(a) Les utilisateurs de signatures électroniques non basées sur la biométrie doivent : (1) recourir à au moins deux méthodes d'identification distinctes, telles qu'un code d'identification et un mot de passe. (i) Lorsqu'une personne exécute une série de signatures lors d'un seul accès continu et contrôlé au système, elle doit apposer la première signature en utilisant tous les composants relatifs à la signature électronique ; les signatures suivantes doivent être apposées à l'aide d'au moins un composant de signature électronique qui ne peut être exécuté que par son propriétaire et généré exclusivement pour celui-ci. (ii) Lorsqu'une personne exécute une ou plusieurs	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	signatures électroniques en dehors d'un seul accès continu et contrôlé au système, elle doit apposer chacune des signatures en utilisant tous les composants relatifs à la signature électronique ; (2) utiliser la signature électronique dont ils sont légitimement propriétaires ; (3) gérer et exécuter les signatures électroniques de manière à garantir que toute tentative d'utilisation d'une signature électronique par un individu autre que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	(a) Les utilisateurs de signatures électroniques non basées sur la biométrie doivent : (1) recourir à au moins deux méthodes d'identification distinctes, telles qu'un code d'identification et un mot de passe. (i) Lorsqu'une personne exécute une série de signatures lors d'un seul accès continu et contrôlé au système, elle doit apposer la première signature en utilisant tous les composants relatifs à la signature électronique ; les signatures suivantes doivent être apposées à l'aide d'au moins un composant de signature électronique qui ne peut être exécuté que par son propriétaire et généré exclusivement pour celui-ci. (ii) Lorsqu'une personne exécute une ou plusieurs	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	signatures électroniques en dehors d'un seul accès continu et contrôlé au système, elle doit apposer chacune des signatures en utilisant tous les composants relatifs à la signature électronique ; (2) utiliser la signature électronique dont ils sont légitimement propriétaires ; (3) gérer et exécuter les signatures électroniques de manière à garantir que toute tentative d'utilisation d'une signature électronique par un individu autre que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	(a) Les utilisateurs de signatures électroniques non basées sur la biométrie doivent : (1) recourir à au moins deux méthodes d'identification distinctes, telles qu'un code d'identification et un mot de passe. (i) Lorsqu'une personne exécute une série de signatures lors d'un seul accès continu et contrôlé au système, elle doit apposer la première signature en utilisant tous les composants relatifs à la signature électronique ; les signatures suivantes doivent être apposées à l'aide d'au moins un composant de signature électronique qui ne peut être exécuté que par son propriétaire et généré exclusivement pour celui-ci. (ii) Lorsqu'une personne exécute une ou plusieurs	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	signatures électroniques en dehors d'un seul accès continu et contrôlé au système, elle doit apposer chacune des signatures en utilisant tous les composants relatifs à la signature électronique ; (2) utiliser la signature électronique dont ils sont légitimement propriétaires ; (3) gérer et exécuter les signatures électroniques de manière à garantir que toute tentative d'utilisation d'une signature électronique par un individu autre que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	(a) Les utilisateurs de signatures électroniques non basées sur la biométrie doivent : (1) recourir à au moins deux méthodes d'identification distinctes, telles qu'un code d'identification et un mot de passe. (i) Lorsqu'une personne exécute une série de signatures lors d'un seul accès continu et contrôlé au système, elle doit apposer la première signature en utilisant tous les composants relatifs à la signature électronique ; les signatures suivantes doivent être apposées à l'aide d'au moins un composant de signature électronique qui ne peut être exécuté que par son propriétaire et généré exclusivement pour celui-ci. (ii) Lorsqu'une personne exécute une ou plusieurs	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	signatures électroniques en dehors d'un seul accès continu et contrôlé au système, elle doit apposer chacune des signatures en utilisant tous les composants relatifs à la signature électronique ; (2) utiliser la signature électronique dont ils sont légitimement propriétaires ; (3) gérer et exécuter les signatures électroniques de manière à garantir que toute tentative d'utilisation d'une signature électronique par un individu autre que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	(a) Les utilisateurs de signatures électroniques non basées sur la biométrie doivent : (1) recourir à au moins deux méthodes d'identification distinctes, telles qu'un code d'identification et un mot de passe. (i) Lorsqu'une personne exécute une série de signatures lors d'un seul accès continu et contrôlé au système, elle doit apposer la première signature en utilisant tous les composants relatifs à la signature électronique ; les signatures suivantes doivent être apposées à l'aide d'au moins un composant de signature électronique qui ne peut être exécuté que par son propriétaire et généré exclusivement pour celui-ci. (ii) Lorsqu'une personne exécute une ou plusieurs	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	signatures électroniques en dehors d'un seul accès continu et contrôlé au système, elle doit apposer chacune des signatures en utilisant tous les composants relatifs à la signature électronique ; (2) utiliser la signature électronique dont ils sont légitimement propriétaires ; (3) gérer et exécuter les signatures électroniques de manière à garantir que toute tentative d'utilisation d'une signature électronique par un individu autre que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.2	(a) Les utilisateurs de signatures électroniques non basées sur la biométrie doivent : (1) recourir à au moins deux méthodes d'identification distinctes, telles qu'un code d'identification et un mot de passe. (i) Lorsqu'une personne exécute une série de signatures lors d'un seul accès continu et contrôlé au système, elle doit apposer la première signature en utilisant tous les composants relatifs à la signature électronique ; les signatures suivantes doivent être apposées à l'aide d'au moins un composant de signature électronique qui ne peut être exécuté que par son propriétaire et généré exclusivement pour celui-ci. (ii) Lorsqu'une personne exécute une ou plusieurs	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	signatures électroniques en dehors d'un seul accès continu et contrôlé au système, elle doit apposer chacune des signatures en utilisant tous les composants relatifs à la signature électronique ; (2) utiliser la signature électronique dont ils sont légitimement propriétaires ; (3) gérer et exécuter les signatures électroniques de manière à garantir que toute tentative d'utilisation d'une signature électronique par un individu autre que son véritable propriétaire nécessite la collaboration de deux personnes ou plus.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	api-gw-cache-enabl ed-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environne ment API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, à partir du moment de leur création jusqu'à leur réception. Ces procédures et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffrement des documents et l'application des normes appropriées en matière de signature numérique afin de garantir, si	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-v ous que le chiffreme nt est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	cmk-backing-key-ro tation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	dynamodb-table-enc rypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffreme nt au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principal e propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	kinesis-stream-enc rypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	kms-cmk-not-schedu led-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	opensearch-encrypt ed-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient, conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confidentialité des enregistrements électroniques, à partir du moment de leur création jusqu'à leur réception. Ces procédures et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffrement des documents et l'application des normes appropriées en matière de signature numérique afin de garantir, si	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	sagemaker-endpoint -configuration-kms- key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	sagemaker-notebook -instance-kms-key- configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-note s, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	secretsmanager-usi ng-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11,3	Les utilisateurs de systèmes ouverts qui créent, modifient , conservent ou transmettent des enregistrements électroniques doivent appliquer les procédures et contrôles conçus pour garantir l'authenticité, l'intégrité et, le cas échéant, la confident ialité des enregistr ements électroniques, à partir du moment de leur création jusqu'à leur réception . Ces procédure s et contrôles doivent inclure ceux mentionnés à la section 11.10, le cas échéant, ainsi que des mesures supplémentaires, telles que le chiffreme nt des documents et l'application des normes approprié es en matière de signature numérique afin de garantir, si	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les circonstances l'exigent, l'authent icité, l'intégrité et la confidentialité des enregistrements.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (b)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure : (b) la garantie que les codes d'identification et les mots de passe délivrés sont périodiquement vérifiés, rappelés ou révisés (par exemple, pour couvrir des événements tels que le vieillissement des mots de passe).	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (b)	Les utilisateurs de signatures électroni ques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure : (b) la garantie que les codes d'identif ication et les mots de passe délivrés sont périodiquement vérifiés, rappelés ou révisés (par exemple, pour couvrir des événements tels que le vieillissement des mots de passe).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (b)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure : (b) la garantie que les codes d'identification et les mots de passe délivrés sont périodiquement vérifiés, rappelés ou révisés (par exemple, pour couvrir des événements tels que le vieillissement des mots de passe).	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (b)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure : (b) la garantie que les codes d'identification et les mots de passe délivrés sont périodiquement vérifiés, rappelés ou révisés (par exemple, pour couvrir des événements tels que le vieillissement des mots de passe).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (b)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure : (b) la garantie que les codes d'identification et les mots de passe délivrés sont périodiquement vérifiés, rappelés ou révisés (par exemple, pour couvrir des événements tels que le vieillissement des mots de passe).	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (b)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure : (b) la garantie que les codes d'identification et les mots de passe délivrés sont périodiquement vérifiés, rappelés ou révisés (par exemple, pour couvrir des événements tels que le vieillissement des mots de passe).	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (d)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure ce qui suit : (d) Prendre des mesures de protection pour sécuriser les transactions dans le but d'empêcher l'utilisation non autorisée des mots de passe et/ou codes d'identification, ainsi que de détecter et de signaler de manière immédiate et prioritaire toute tentative d'utilisation non autorisée à l'unité de sécurité du système et, le cas échéant, à l'équipe de gestion organisationnelle.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (d)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure ce qui suit : (d) Prendre des mesures de protection pour sécuriser les transactions dans le but d'empêcher l'utilisation non autorisée des mots de passe et/ou codes d'identification, ainsi que de détecter et de signaler de manière immédiate et prioritaire toute tentative d'utilisation non autorisée à l'unité de sécurité du système et, le cas échéant, à l'équipe de gestion organisationnelle.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (d)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure ce qui suit : (d) Prendre des mesures de protection pour sécuriser les transactions dans le but d'empêcher l'utilisation non autorisée des mots de passe et/ou codes d'identification, ainsi que de détecter et de signaler de manière immédiate et prioritaire toute tentative d'utilisation non autorisée à l'unité de sécurité du système et, le cas échéant, à l'équipe de gestion organisationnelle.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.300 (d)	Les utilisateurs de signatures électroniques exigeant un code d'identification et un mot de passe doivent appliquer des mesures de contrôle afin de garantir la sécurité et l'intégrité du processus. Ces contrôles doivent inclure ce qui suit : (d) Prendre des mesures de protection pour sécuriser les transactions dans le but d'empêcher l'utilisation non autorisée des mots de passe et/ou codes d'identification, ainsi que de détecter et de signaler de manière immédiate et prioritaire toute tentative d'utilisation non autorisée à l'unité de sécurité du système et, le cas échéant, à l'équipe de gestion organisationnelle.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for FDA Title 21 CFR Part 11.

Bonnes pratiques de fonctionnement pour FedRAMP(Low)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les contrôles de base faibles du Federal Risk and Authorization Management Program (FedRAMP) et les règles de configuration AWS gérées. Chaque règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles FedRAMP. Un contrôle FedRAMP peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC-2	GESTION DE COMPTE	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-2	GESTION DE COMPTE	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC-2	GESTION DE COMPTE	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	GESTION DE COMPTE	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
AC-3	EXÉCUTION D'ACCÈS	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
AC-3	EXÉCUTION D'ACCÈS	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-3	EXÉCUTION D'ACCÈS	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-3	EXÉCUTION D'ACCÈS	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-3	EXÉCUTION D'ACCÈS	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	EXÉCUTION D'ACCÈS	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
AC-3	ACCÈS DISTANT	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-3	ACCÈS DISTANT	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
AC-3	ACCÈS DISTANT	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-3	ACCÈS DISTANT	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-3	ACCÈS DISTANT	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
AC-3	ACCÈS DISTANT	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-3	ACCÈS DISTANT	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-3	ACCÈS DISTANT	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	ACCÈS DISTANT	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-2	ÉVÉNEMENTS D'AUDIT	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-2	ÉVÉNEMENTS D'AUDIT	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	ÉVÉNEMENTS D'AUDIT	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTR EMENTS D'AUDIT	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTR EMENTS D'AUDIT	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTREMENTS D'AUDIT	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTR EMENTS D'AUDIT	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	CONTENU DES ENREGISTR EMENTS D'AUDIT	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6	EXAMEN, ANALYSE ET RAPPORTS D'AUDIT	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	PROTECTION DES INFORMATIONS D'AUDIT	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
AU-9	PROTECTION DES INFORMATIONS D'AUDIT	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	PROTECTION DES INFORMATIONS D'AUDIT	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	PROTECTION DES INFORMATIONS D'AUDIT	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	PROTECTION DES INFORMATIONS D'AUDIT	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-11	CONSERVATION DES ENREGISTREMENTS D'AUDIT	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-12	OPÉRATION D'AUDIT	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-12	OPÉRATION D'AUDIT	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	OPÉRATION D'AUDIT	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
CA-7	SURVEILLANCE CONTINUE	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CA-7	SURVEILLANCE CONTINUE	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	SURVEILLANCE CONTINUE	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM-2	CONFIGURATION DE RÉFÉRENCE	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CM-2	CONFIGURATION DE RÉFÉRENCE	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CM-2	CONFIGURATION DE RÉFÉRENCE	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CM-2	CONFIGURATION DE RÉFÉRENCE	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM-2	CONFIGURATION DE RÉFÉRENCE	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	CONFIGURATION DE RÉFÉRENCE	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
CM-7	PRINCIPE DE MOINDRE FONCTIONNALITÉ	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-7	PRINCIPE DE MOINDRE FONCTIONNALITÉ	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-7	PRINCIPE DE MOINDRE FONCTIONNALITÉ	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8	INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8	INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8	INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8	INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CP-9	BACKUP DU SYSTÈME D'INFORMATION	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	BACKUP DU SYSTÈME D'INFORMATION	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	REPRISE ET RECONSTITUTION DU SYSTÈME D'INFORMATION	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DE L'ORGANISATION)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DE L'ORGANISATION)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DE L'ORGANISATION)	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DE L'ORGANISATION)	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DE L'ORGANISATION)	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS DE L'ORGANISATION)	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	GESTION DES AUTHENTIF ICATIONS	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	GESTION DES AUTHENTIF ICATIONS	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4	GESTION DES INCIDENTS	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4	GESTION DES INCIDENTS	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4	GESTION DES INCIDENTS	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4	GESTION DES INCIDENTS	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4	GESTION DES INCIDENTS	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-6	SIGNALEMENT D'INCIDENTS	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-6	SIGNALEMENT D'INCIDENTS	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-6	SIGNALEMENT D'INCIDENTS	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-7	ASSISTANCE POUR LA RÉPONSE AUX INCIDENTS	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-7	ASSISTANCE POUR LA RÉPONSE AUX INCIDENTS	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-7	ASSISTANCE POUR LA RÉPONSE AUX INCIDENTS	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5	ANALYSE DES VULNÉRABILITÉS	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5	ANALYSE DES VULNÉRABILITÉS	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5	ANALYSE DES VULNÉRABILITÉS	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-3	CYCLE DE VIE DU DÉVELOPPEMENT DU SYSTÈME	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-3	CYCLE DE VIE DU DÉVELOPPEMENT DU SYSTÈME	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-3	CYCLE DE VIE DU DÉVELOPPEMENT DU SYSTÈME	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	PROTECTION CONTRE LE DÉNI DE SERVICE	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
SC-7	PROTECTION DES LIMITES	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7	PROTECTION DES LIMITES	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-7	PROTECTION DES LIMITES	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7	PROTECTION DES LIMITES	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC-7	PROTECTION DES LIMITES	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7	PROTECTION DES LIMITES	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-7	PROTECTION DES LIMITES	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	PROTECTION DES LIMITES	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.
SC-12	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	PROTECTION PAR LE CHIFFREMENT	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	PROTECTION PAR LE CHIFFREMENT	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC-13	PROTECTION PAR LE CHIFFREMENT	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	PROTECTION PAR LE CHIFFREMENT	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	PROTECTION PAR LE CHIFFREMENT	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	PROTECTION PAR LE CHIFFREMENT	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	CORRECTION DES FAILLES	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	CORRECTION DES FAILLES	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	CORRECTION DES FAILLES	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	CORRECTION DES FAILLES	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3	CORRECTION DES FAILLES	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3	CORRECTION DES FAILLES	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
SI-3	CORRECTION DES FAILLES	ecs-task-definition-memory-hard-limit	Limiter la mémoire maximale disponibl e sur vos conteneur s Amazon Elastic Container Service (ECS) garantit que vos ressources ne peuvent pas être utilisées de manière abusive en cas d'accès malveillant à vos conteneurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	SURVEILLANCE DU SYSTÈME D'INFORMATION	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	ALERTES, CONSEILS ET DIRECTIVES DE SÉCURITÉ	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	ALERTES, CONSEILS ET DIRECTIVES DE SÉCURITÉ	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	ALERTES, CONSEILS ET DIRECTIVES DE SÉCURITÉ	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	ALERTES, CONSEILS ET DIRECTIVES DE SÉCURITÉ	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	GESTION ET CONSERVATION DES INFORMATIONS	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-16	PROTECTION DE LA MÉMOIRE	ecs-task-definition-memory-hard-limit	Limiter la mémoire maximale disponible sur vos conteneurs Amazon Elastic Container Service (ECS) garantit que vos ressources ne peuvent pas être utilisées de manière abusive en cas d'accès malveillant à vos conteneurs.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for FedRAMP (Low).

Bonnes pratiques de fonctionnement pour FedRAMP (modérée)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Federal Risk and Authorization Management Program (FedRAMP) et les règles de configuration AWS gérées. Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles FedRAMP. Un contrôle FedRAMP peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Ce pack de conformité a été validé par AWS Security Assurance Services LLC (AWS SAS), qui est une équipe d'évaluateurs de sécurité qualifiés (QSA) dans le secteur des cartes de paiement, de

praticiens certifiés par HITRUST Common Security Framework (CCSFP) et de professionnels de la conformité certifiés pour fournir des conseils et des évaluations pour divers frameworks industriels. AWS Les professionnels de SAS ont conçu ce pack de conformité pour permettre à un client de s'aligner sur un sous-ensemble des contrôles FedRAMP.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(3)	Le système d'information désactive automatiquement les comptes utilisateurs inactifs au bout de 90 jours.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(3)	Le système d'information désactive automatiquement les comptes utilisateurs inactifs au bout de 90 jours.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(7)	L'organisation : (a) définit et gère les utilisateurs privilégiés conformément à un schéma d'accès basé sur les rôles qui détermine l'accès autorisé au système d'information et les privilèges de chaque rôle ; (b) surveille les attributions de rôles privilégiés ; et (c) effectue [Attribution : actions définies par l'organisation] si les attributions de rôles privilégiés ne sont plus appropriées. Conseils supplémentaires : les rôles privilégiés sont des rôles définis par l'organisation et attribués à des individus, permettant à ces derniers d'exécuter certaines fonctions de sécurité que les utilisateurs ordinaires ne sont pas autorisés à exécuter. Ces rôles privilégiés	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	incluent, par exemple, la gestion des clés, la gestion des comptes, l'administration réseau et système, l'administration des bases de données et l'administration Web.		refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(7)	L'organisation : (a) définit et gère les utilisateurs privilégiés conformément à un schéma d'accès basé sur les rôles qui détermine l'accès autorisé au système d'information et les privilèges de chaque rôle ; (b) surveille les attributions de rôles privilégiés ; et (c) effectue [Attribution : actions définies par l'organisation] si les attributions de rôles privilégiés ne sont plus appropriées. Conseils supplémentaires : les rôles privilégiés sont des rôles définis par l'organisation et attribués à des individus, permettant à ces derniers d'exécuter certaines fonctions de sécurité que les utilisateurs ordinaires ne sont pas autorisés à exécuter. Ces rôles privilégiés	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	incluent, par exemple, la gestion des clés, la gestion des comptes, l'administration réseau et système, l'administration des bases de données et l'administration Web.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(7)	L'organisation : (a) définit et gère les utilisateurs privilégiés conformément à un schéma d'accès basé sur les rôles qui détermine l'accès autorisé au système d'information et les privilèges de chaque rôle ; (b) surveille les attributions de rôles privilégiés ; et (c) effectue [Attribution : actions définies par l'organisation] si les attributions de rôles privilégiés ne sont plus appropriées. Conseils supplémentaires : les rôles privilégiés sont des rôles définis par l'organisation et attribués à des individus, permettant à ces derniers d'exécuter certaines fonctions de sécurité que les utilisateurs ordinaires ne sont pas autorisés à exécuter. Ces rôles privilégiés	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	incluent, par exemple, la gestion des clés, la gestion des comptes, l'administration réseau et système, l'administration des bases de données et l'administration Web.		refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(7)	L'organisation : (a) définit et gère les utilisateurs privilégiés conformément à un schéma d'accès basé sur les rôles qui détermine l'accès autorisé au système d'information et les privilèges de chaque rôle ; (b) surveille les attributions de rôles privilégiés ; et (c) effectue [Attribution : actions définies par l'organisation] si les attributions de rôles privilégiés ne sont plus appropriées. Conseils supplémentaires : les rôles privilégiés sont des rôles définis par l'organisation et attribués à des individus, permettant à ces derniers d'exécuter certaines fonctions de sécurité que les utilisateurs ordinaires ne sont pas autorisés à exécuter. Ces rôles privilégiés	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	incluent, par exemple, la gestion des clés, la gestion des comptes, l'administration réseau et système, l'administration des bases de données et l'administration Web.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(7)	L'organisation : (a) définit et gère les utilisateurs privilégiés conformément à un schéma d'accès basé sur les rôles qui détermine l'accès autorisé au système d'information et les privilèges de chaque rôle ; (b) surveille les attributions de rôles privilégiés ; et (c) effectue [Attribution : actions définies par l'organisation] si les attributions de rôles privilégiés ne sont plus appropriées. Conseils supplémentaires : les rôles privilégiés sont des rôles définis par l'organisation et attribués à des individus, permettant à ces derniers d'exécuter certaines fonctions de sécurité que les utilisateurs ordinaires ne sont pas autorisés à exécuter. Ces rôles privilégiés	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	incluent, par exemple, la gestion des clés, la gestion des comptes, l'administration réseau et système, l'administration des bases de données et l'administration Web.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(7)	L'organisation : (a) définit et gère les utilisateurs privilégiés conformément à un schéma d'accès basé sur les rôles qui détermine l'accès autorisé au système d'information et les privilèges de chaque rôle ; (b) surveille les attributions de rôles privilégiés ; et (c) effectue [Attribution : actions définies par l'organisation] si les attributions de rôles privilégiés ne sont plus appropriées. Conseils supplémentaires : les rôles privilégiés sont des rôles définis par l'organisation et attribués à des individus, permettant à ces derniers d'exécuter certaines fonctions de sécurité que les utilisateurs ordinaires ne sont pas autorisés à exécuter. Ces rôles privilégiés	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	incluent, par exemple, la gestion des clés, la gestion des comptes, l'administration réseau et système, l'administration des bases de données et l'administration Web.		
AC-2(12)(a)	L'organisation : a. Surveille les comptes du système d'informa tion pour [Attribution : utilisation atypique définie par l'organis ation].	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(12)(a)	L'organisation : a. Surveille les comptes du système d'information pour [Attribution : utilisation atypique définie par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant l'authent ification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisat ions d'accès au système d'informa tion pour faciliter la séparation des tâches.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
AC-6(10)	Le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, notamment de désactiver, de contourner ou de modifier les mesures/contre-mesures de sécurité mises en œuvre.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6(10)	Le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, notamment de désactiver, de contourner ou de modifier les mesures/contre-mesures de sécurité mises en œuvre.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6(10)	Le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, notamment de désactiver, de contourner ou de modifier les mesures/contre-mesures de sécurité mises en œuvre.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild . AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège, en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège, en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	sagemaker-notebook -no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'administrateur, des contrôles d'authentification, des contrôles d'autorisation, des suppressions de données, des accès aux données, des modifications de données et des modifications d'autorisations. d. Détermine que les événements suivants doivent être audités dans le système d'informa	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	wafv2-logging-enab led	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'administrateur, des contrôles d'authentification, des contrôles d'autorisation, des suppressions de données, des accès aux données, des modifications de données et des modifications d'autorisations. d. Détermine que les événements suivants doivent être audités dans le système d'informa	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : événements de réussite et d'échec d'ouverture de compte, événements de gestion de compte, accès aux objets, modification des politiques, fonctions privilégiées, suivi des processus et événements système. Pour les applications Web : l'ensemble des activités de l'adminis trateur, des contrôles d'authentification, des contrôles d'autoris ation, des suppressi ons de données, des accès aux données, des modifications de données et des modifications d'autoris ations. d. Détermine que les événement s suivants doivent être audités dans le système d'informa	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tion : [sous-ensemble des événements vérifiables définis dans AU-2 a défini par l'organisation devant être constamment audité pour chaque événement identifié].		
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-7(1)	Le système d'information permet de traiter les enregistrements d'audit pour les événements intéressants en fonction de [Attribution : champs d'audit définis par l'organisation dans les enregistrements d'audit].	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-7(1)	Le système d'information permet de traiter les enregistrements d'audit pour les événements intéressants en fonction de [Attribution : champs d'audit définis par l'organisation dans les enregistrements d'audit].	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9(2)	Le système d'information sauvegarde les enregistrements d'audit au moins une fois par semaine sur un système ou un composant du système physiquement différent du système ou du composant vérifié.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9(2)	Le système d'information sauvegarde les enregistrements d'audit au moins une fois par semaine sur un système ou un composant du système physiquement différent du système ou du composant vérifié.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	Le système d'information protège les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	Le système d'information protège les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	Le système d'information protège les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
AU-11	L'organisation conserve les dossiers d'audit pendant au moins 90 jours afin de soutenir les after-the-fact enquêtes sur les incidents de sécurité et de répondre aux exigences réglementaires et organisationnelles en matière de conservation des informations.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. sur tous les composants du système d'information et du réseau où la capacité d'audit est déployée/disponible c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveilla nce et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveilla nce et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveilla nce et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveilla nce et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
CM-7(a)	L'organisation : a. Configure le système d'information pour qu'il ne fournisse que les fonctionnalités essentielles.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-7(a)	L'organisation : a. Configure le système d'information pour qu'il ne fournisse que les fonctionnalités essentielles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-7(a)	L'organisation : a. Configure le système d'information pour qu'il ne fournisse que les fonctionnalités essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8(1)	L'organisation met à jour l'inventaire des composants du système d'information en tant que partie intégrante des installations, des suppressions et des mises à jour du système d'information.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8(1)	L'organisation met à jour l'inventaire des composants du système d'information en tant que partie intégrante des installations, des suppressions et des mises à jour du système d'information.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8(3)(a)	L'organisation : a. Utilise des mécanismes automatisés en continu qui présentent un délai maximal de cinq minutes pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8(3)(a)	L'organisation : a. Utilise des mécanismes automatisés en continu qui présentent un délai maximal de cinq minutes pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8(3)(a)	L'organisation : a. Utilise des mécanismes automatisés en continu qui présentent un délai maximal de cinq minutes pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8(3)(a)	L'organisation : a. Utilise des mécanismes automatisés en continu qui présenten t un délai maximal de cinq minutes pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrémentielle tous les jours ; entièrement toutes les semaines).	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrémentielle tous les jours ; entièrement toutes les semaines).	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrémentielle tous les jours ; entièrement toutes les semaines).	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	efs-resources-prot ected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrémentielle tous les jours ; entièrement toutes les semaines).	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9(b)	L'organisation : b. Sauvegardes les informations du système contenues dans le système d'information (de manière incrément ielle tous les jours ; entièrement toutes les semaines).	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)(2)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (2) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)(2)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (2) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)(2)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (2) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)(2)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (2) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes non privilégiés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)	(1) Le système d'information met en œuvre une authentif ication multifactorielle pour l'accès réseau aux comptes privilégi és.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2(1)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	Le système d'information identifie et authentifie de manière unique les utilisateurs de l'organisation (ou les processus agissant pour le compte des utilisateurs de l'organisation).	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2	Le système d'information identifie et authentifie de manière unique les utilisateurs de l'organisation (ou les processus agissant pour le compte des utilisateurs de l'organisation).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5(1)(a)(d)(e)	Le système d'information, pour l'authentification par mot de passe : a. Applique une complexité minimale des mots de passe de [Attribution : exigences définies par l'organisation pour la sensibilité à la casse, le nombre de caractères, la combinaison de lettres majuscules, de lettres minuscules, de chiffres et de caractères spéciaux, y compris les exigences minimales pour chaque type] ; d. Applique des restrictions de durée de vie minimale et maximale des mots de passe de [Attribution : nombres définis par l'organisation pour la durée de vie minimale, la durée de vie maximale] ; e. Interdit la réutilisation des mots de passe pendant 24 générations	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5(4)	L'organisation utilise des outils automatis és pour détermine r si les authentif icateurs de mots de passe sont suffisamm ent puissants pour satisfaire [Attribution : exigences définies par l'organisation].	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5(7)	L'organisation veille à ce que les authentificateurs statiques non chiffrés ne soient pas intégrés à des applications ou des scripts d'accès, ni stockés sur des touches de fonction.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4(1)	L'organisation utilise des mécanismes automatisés pour faciliter le processus de gestion des incidents.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4(1)	L'organisation utilise des mécanismes automatisés pour faciliter le processus de gestion des incidents.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4(1)	L'organisation utilise des mécanismes automatisés pour faciliter le processus de gestion des incidents.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4(1)	L'organisation utilise des mécanismes automatisés pour faciliter le processus de gestion des incidents.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4(1)	L'organisation utilise des mécanismes automatisés pour faciliter le processus de gestion des incidents.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-6(1)	L'organisation utilise des mécanismes automatisés pour faciliter le signalement des incidents de sécurité.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-6(1)	L'organisation utilise des mécanismes automatisés pour faciliter le signalement des incidents de sécurité.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-6(1)	L'organisation utilise des mécanismes automatisés pour faciliter le signalement des incidents de sécurité.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-7(1)	L'organisation utilise des mécanismes automatisés pour améliorer la disponibilité des informations et de la prise en charge liées à la réponse aux incidents.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-7(1)	L'organisation utilise des mécanismes automatisés pour améliorer la disponibilité des informations et de la prise en charge liées à la réponse aux incidents.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-7(1)	L'organisation utilise des mécanismes automatisés pour améliorer la disponibilité des informations et de la prise en charge liées à la réponse aux incidents.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5(1)	L'organisation utilise des outils d'analyse des vulnérabilités qui permettent notamment d'immédiatement détecter les vulnérabilités du système d'information à analyser. Conseils supplémentaires : les vulnérabilités à analyser doivent être mises à jour dès que de nouvelles vulnérabilités sont détectées et annoncées, et que des méthodes d'analyse sont développées. Ce processus de mise à jour permet de s'assurer que les potentielles vulnérabilités du système d'information sont identifiées et corrigées le plus rapidement possible. Contrôles associés : SI-3, SI-7.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5(1)	L'organisation utilise des outils d'analyse des vulnérabilités qui permettent notamment d'immédiatement détecter les vulnérabilités du système d'information à analyser. Conseils supplémentaires : les vulnérabilités à analyser doivent être mises à jour dès que de nouvelles vulnérabilités sont détectées et annoncées, et que des méthodes d'analyse sont développées. Ce processus de mise à jour permet de s'assurer que les potentielles vulnérabilités du système d'information sont identifiées et corrigées le plus rapidement possible. Contrôles associés : SI-3, SI-7.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5(1)	L'organisation utilise des outils d'analyse des vulnérabilités qui permettent notamment d'immédiatement détecter les vulnérabilités du système d'information à analyser. Conseils supplémentaires : les vulnérabilités à analyser doivent être mises à jour dès que de nouvelles vulnérabilités sont détectées et annoncées, et que des méthodes d'analyse sont développées. Ce processus de mise à jour permet de s'assurer que les potentielles vulnérabilités du système d'information sont identifiées et corrigées le plus rapidement possible. Contrôles associés : SI-3, SI-7.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5	L'organisation : a. Analyse chaque mois les vulnérabilités du système d'information et des applications hébergées [système/infrastructure d'exploitation ; applications Web et bases de données mensuelles], et dès que de nouvelles vulnérabilités susceptibles d'affecter le système/les applications sont identifiées et signalées ; b. Utilise des outils et des techniques d'analyse des vulnérabilités qui facilitent l'interopérabilité entre les outils et automatisent certaines parties du processus de gestion des vulnérabilités en utilisant des normes pour : 1. L'énumération des plateformes, des failles logicielles et des configurations inappropriées ; 2. Le formatage des listes	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de contrôle et des procédures de test ; et 3. La mesure de l'impact des vulnérabilités ; c. Analyse les rapports d'analyse des vulnérabilités et les résultats des évaluations de contrôle de la sécurité ; d. Corrige les vulnérabilités légitimes : vulnérabilités à haut risque atténuées dans les trente (30) jours suivant la date de détection ; vulnérabilités à risque modéré atténuées dans les quatre-vingt-dix (90) jours suivant la date de détection ; vulnérabilités à faible risque atténuées dans les cent quatre-vingts (180) jours suivant la date de détection , selon une évaluation des risques menée par l'organisation ; et e. Partage les informations obtenues dans le cadre du		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	processus d'analyse des vulnérabilités et des évaluations de contrôle de la sécurité avec [Attribution : personnel ou rôles définis par l'organisation] pour faciliter l'élimination des vulnérabilités similaires dans d'autres systèmes d'information (c'est-à-dire les faiblesses ou déficiences systémiques).		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5	L'organisation : a. Recherche les vulnérabilités dans le système d'information et les applications hébergées [Attribution : fréquence définie par l'organisation et/ou de manière aléatoire conformément au processus défini par l'organisation] et lorsque de nouvelles vulnérabilités susceptibles d'affecter le système/les applications sont identifiées et signalées ; b. Utilise des outils et des techniques d'analyse des vulnérabilités qui facilitent l'interopérabilité entre les outils et automatisent certaines parties du processus de gestion des vulnérabilités en utilisant des normes pour : 1. L'énumération des plateformes, des failles logicielles et des configurations	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	inappropriées ; 2. Le formatage des listes de contrôle et des procédures de test ; et 3. La mesure de l'impact des vulnérabilités ; c. Analyse les rapports d'analyse des vulnérabilités et les résultats des évaluations de contrôle de la sécurité ; d. Corrige les vulnérabilités légitimes [Attribution : temps de réponse définis par l'organisation], conformément à une évaluation organisationnelle des risques ; et e. Partage les informations obtenues dans le cadre du processus d'analyse des vulnérabilités et des évaluations de contrôle de la sécurité avec [Attribution : personnel ou rôles définis par l'organisation] pour faciliter l'élimination des vulnérabi		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	lités similaires dans d'autres systèmes d'information (c'est-à-dire les faiblesses ou déficiences systémiques).		
SA-3(a)	L'organisation : a. Gère le système d'information en utilisant [Attribution : cycle de vie du développement du système défini par l'organisation] qui intègre des considérations relatives à la sécurité de l'information.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-3(a)	L'organisation : a. Gère le système d'information en utilisant [Attribution : cycle de vie du développement du système défini par l'organisation] qui intègre des considérations relatives à la sécurité de l'information.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-3(a)	L'organisation : a. Gère le système d'information en utilisant [Attribution : cycle de vie du développement du système défini par l'organisation] qui intègre des considérations relatives à la sécurité de l'information.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10	L'organisation exige que le développeur du système d'information, du composant du système ou du service du système d'information : a. Gère la configuration lors du développement, de la mise en œuvre ET de l'exploitation du système, des composants ou des services ; b. Documente, gère et contrôle l'intégrité des modifications apportées à [Attribution : éléments de configuration définis par l'organisation dans le cadre de la gestion de la configuration] ; c. Mette en œuvre uniquement les modifications approuvées par l'organisation dans le système, le composant ou le service ; d. Documente	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10	L'organisation exige que le développeur du système d'informa tion, du composant du système ou du service du système d'information : a. Gère la configuration lors du développe ment, de la mise en œuvre ET de l'exploit ation du système, des composants ou des services ; b. Documente, gère et contrôle l'intégri té des modificat ions apportées à [Attribution : éléments de configura tion définis par l'organisation dans le cadre de la gestion de la configura tion] ; c. Mette en œuvre uniquemen t les modificat ions approuvées par l'organisation dans le système, le composant ou le service ; d. Documente	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10	L'organisation exige que le développeur du système d'information, du composant du système ou du service du système d'information : a. Gère la configuration lors du développement, de la mise en œuvre ET de l'exploitation du système, des composants ou des services ; b. Documente, gère et contrôle l'intégrité des modifications apportées à [Attribution : éléments de configuration définis par l'organisation dans le cadre de la gestion de la configuration] ; c. Mette en œuvre uniquement les modifications approuvées par l'organisation dans le système, le composant ou le service ; d. Documente	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10	L'organisation exige que le développeur du système d'informa tion, du composant du système ou du service du système d'information : a. Gère la configuration lors du développe ment, de la mise en œuvre ET de l'exploit ation du système, des composants ou des services ; b. Documente, gère et contrôle l'intégri té des modificat ions apportées à [Attribution : éléments de configura tion définis par l'organisation dans le cadre de la gestion de la configura tion] ; c. Mette en œuvre uniquemen t les modificat ions approuvées par l'organisation dans le système, le composant ou le service ; d. Documente	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-2	Le système d'information sépare les fonctionnalités utilisateur (y compris les services d'interface utilisateur) des fonctionnalités de gestion du système d'information.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-2	Le système d'information sépare les fonctionnalités utilisateur (y compris les services d'interface utilisateur) des fonctionnalités de gestion du système d'information.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-2	Le système d'information sépare les fonctionnalités utilisateur (y compris les services d'interface utilisateur) des fonctionnalités de gestion du système d'information.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-2	Le système d'information sépare les fonctionnalités utilisateur (y compris les services d'interface utilisateur) des fonctionnalités de gestion du système d'information.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-2	Le système d'information sépare les fonctionnalités utilisateur (y compris les services d'interface utilisateur) des fonctionnalités de gestion du système d'information.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexion s réseau externes au système d'informa tion.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(4)	L'organisation : (a) implémente une interface gérée pour chaque service de télécommunication externe ; (b) établit une politique de flux de trafic pour chaque interface gérée ; (c) protège la confident ialité et l'intégrité des informations transmises via chaque interface ; (d) justifie à l'aide de documents chaque exception à la politique de flux de trafic par une mission/ un besoin de l'entepr ise sous-jacent(e) en indiquant la durée de ce besoin ; et (e) examine les exception s à la politique de flux de trafic [Attribut ion : fréquence définie par l'organisation] et supprime les exceptions qui ne sont plus justifiée s par une mission explicite/un besoin de l'entreprise. Conseils	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : contrôle associé : SC-8.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(4)	L'organisation : (a) implémente une interface gérée pour chaque service de télécommunication externe ; (b) établit une politique de flux de trafic pour chaque interface gérée ; (c) protège la confidentialité et l'intégrité des informations transmises via chaque interface ; (d) justifie à l'aide de documents chaque exception à la politique de flux de trafic par une mission/un besoin de l'entreprise sous-jacent(e) en indiquant la durée de ce besoin ; et (e) examine les exceptions à la politique de flux de trafic [Attribution : fréquence définie par l'organisation] et supprime les exceptions qui ne sont plus justifiées par une mission explicite/un besoin de l'entreprise. Conseils	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : contrôle associé : SC-8.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(4)	L'organisation : (a) implémente une interface gérée pour chaque service de télécommunication externe ; (b) établit une politique de flux de trafic pour chaque interface gérée ; (c) protège la confident ialité et l'intégrité des informations transmises via chaque interface ; (d) justifie à l'aide de documents chaque exception à la politique de flux de trafic par une mission/ un besoin de l'entepr ise sous-jacent(e) en indiquant la durée de ce besoin ; et (e) examine les exception s à la politique de flux de trafic [Attribut ion : fréquence définie par l'organisation] et supprime les exceptions qui ne sont plus justifiée s par une mission explicite/un besoin de l'entreprise. Conseils	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : contrôle associé : SC-8.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(4)	L'organisation : (a) implémente une interface gérée pour chaque service de télécommunication externe ; (b) établit une politique de flux de trafic pour chaque interface gérée ; (c) protège la confident ialité et l'intégrité des informations transmises via chaque interface ; (d) justifie à l'aide de documents chaque exception à la politique de flux de trafic par une mission/ un besoin de l'entepr ise sous-jacent(e) en indiquant la durée de ce besoin ; et (e) examine les exception s à la politique de flux de trafic [Attribut ion : fréquence définie par l'organisation] et supprime les exceptions qui ne sont plus justifiée s par une mission explicite/un besoin de l'entreprise. Conseils	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : contrôle associé : SC-8.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(4)	L'organisation : (a) implémente une interface gérée pour chaque service de télécommunication externe ; (b) établit une politique de flux de trafic pour chaque interface gérée ; (c) protège la confident ialité et l'intégrité des informations transmises via chaque interface ; (d) justifie à l'aide de documents chaque exception à la politique de flux de trafic par une mission/ un besoin de l'entepr ise sous-jacent(e) en indiquant la durée de ce besoin ; et (e) examine les exception s à la politique de flux de trafic [Attribut ion : fréquence définie par l'organisation] et supprime les exceptions qui ne sont plus justifiée s par une mission explicite/un besoin de l'entreprise. Conseils	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : contrôle associé : SC-8.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7(4)	L'organisation : (a) implémente une interface gérée pour chaque service de télécommunication externe ; (b) établit une politique de flux de trafic pour chaque interface gérée ; (c) protège la confident ialité et l'intégrité des informations transmises via chaque interface ; (d) justifie à l'aide de documents chaque exception à la politique de flux de trafic par une mission/ un besoin de l'entepr ise sous-jacent(e) en indiquant la durée de ce besoin ; et (e) examine les exception s à la politique de flux de trafic [Attribut ion : fréquence définie par l'organisation] et supprime les exceptions qui ne sont plus justifiée s par une mission explicite/un besoin de l'entreprise. Conseils	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : contrôle associé : SC-8.		
SC-7(5)	Au niveau des interfaces gérées, le système d'informa tion refuse le trafic de communications réseau par défaut et autorise le trafic de communications réseau par exception (c'est-à-dire, tout refuser, autoriser par exception). Conseils supplémen taires : ce contrôle amélioré s'applique à la fois aux trafics de communications réseau entrant et sortant. Une politique de refus de tout trafic de communications permit-by-exception réseau garantit que seules les connexion s essentielles et approuvées sont autorisées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Le système d'information protège la confidentialité ET l'intégrité des informations transmises.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Le système d'information protège la confidentialité ET l'intégrité des informations transmises.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-8	Le système d'information protège la confidentialité ET l'intégrité des informations transmises.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Le système d'information protège la confidentialité ET l'intégrité des informations transmises.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8	Le système d'information protège la confidentialité ET l'intégrité des informations transmises.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Le système d'information protège la confidentialité ET l'intégrité des informations transmises.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8	Le système d'information protège la confidentialité ET l'intégrité des informations transmises.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12	L'organisation établit et gère les clés de chiffrement nécessaires au chiffrement employé dans le système d'information conformément à [Attribution : exigences définies par l'organisation pour la génération, la distribution, le stockage, l'accès et la destruction des clés].	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.
SC-12	L'organisation établit et gère les clés de chiffrement nécessaires au chiffrement employé dans le système d'information conformément à [Attribution : exigences définies par l'organisation pour la génération, la distribution, le stockage, l'accès et la destruction des clés].	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12	L'organisation établit et gère les clés de chiffrement nécessaires au chiffrement employé dans le système d'information conformément à [Attribution : exigences définies par l'organisation pour la génération, la distribution, le stockage, l'accès et la destruction des clés].	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Le système d'information met en œuvre un chiffrement validé par les FIPS ou approuvé par la NSA, conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements et aux normes applicables.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Le système d'information met en œuvre un chiffrement validé par les FIPS ou approuvé par la NSA, conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements et aux normes applicables.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC-13	Le système d'information met en œuvre un chiffrement validé par les FIPS ou approuvé par la NSA, conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements et aux normes applicables.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Le système d'information met en œuvre un chiffrement validé par les FIPS ou approuvé par la NSA, conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements et aux normes applicables.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Le système d'information met en œuvre un chiffrement validé par les FIPS ou approuvé par la NSA, conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements et aux normes applicables.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Le système d'information met en œuvre un chiffrement validé par les FIPS ou approuvé par la NSA, conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements et aux normes applicables.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Le système d'information protège l'authenticité des sessions de communication.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23	Le système d'information protège l'authenticité des sessions de communication.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Le système d'information protège l'authenticité des sessions de communication.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23	Le système d'information protège l'authenticité des sessions de communication.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Le système d'information protège l'authenticité des sessions de communication.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23	Le système d'information protège l'authenticité des sessions de communication.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Le système d'information protège la confidentialité ET l'intégrité des [Attribution : informations au repos définies par l'organisation].	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2(2)	L'organisation utilise des mécanismes automatisés au moins une fois par mois pour déterminer l'état des composants du système d'information en ce qui concerne la correction des failles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2(2)	L'organisation utilise des mécanismes automatisés au moins une fois par mois pour déterminer l'état des composants du système d'information en ce qui concerne la correction des failles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2(2)	L'organisation utilise des mécanismes automatisés au moins une fois par mois pour déterminer l'état des composants du système d'information en ce qui concerne la correction des failles.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2(2)	L'organisation utilise des mécanismes automatisés au moins une fois par mois pour déterminer l'état des composants du système d'information en ce qui concerne la correction des failles.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3	L'organisation : a. Utilise des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie du système d'information pour détecter et éradiquer les codes malveillants ; b. Met à jour les mécanismes de protection contre les codes malveillants dès que de nouvelles versions sont disponibles conformément aux politiques et procédures de gestion de la configuration de l'entreprise ; c. Configure les mécanismes de protection contre les codes malveillants pour : 1. Effectuer des analyses périodiques du système d'information [Attribution : fréquence définie par l'organisation] et des analyses en temps	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild . AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	réel des fichiers provenant de sources externes sur [Sélection (un ou plusieurs) ; point de terminaison ; points d'entrée/sortie du réseau] lorsque les fichiers sont téléchargés, ouverts ou exécutés conformément à la politique de sécurité de l'entreprise ; et 2. [Sélection (un ou plusieurs) : Bloquer le code malveillant ; Mettre le code malveillant en quarantaine ; Envoyer une alerte à l'administrateur ; [Attribution : action définie par l'organisation]] après la détection d'un code malveillant ; et d. Répond aux faux positifs lors de la détection et de l'éradication des codes malveillants et à l'impact potentiel qui en résulte sur la disponibilité du système d'information. Conseils		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : les points d'entrée et de sortie des systèmes d'information incluent, par exemple, les pare-feu, les serveurs de messagerie électronique, les serveurs Web, les serveurs proxy, les serveurs d'accès à distance, les stations de travail, les ordinateurs portables et les appareils mobiles. Les codes malveillants comprennent notamment les virus, les vers, les chevaux de Troie et les logiciels espions. Le code malveillant peut également être codé dans différents formats (par exemple, UUENCODE, Unicode), contenu dans des fichiers compressés ou masqués, ou masqué dans des fichiers à l'aide de la stéganographie. Les codes malveillants peuvent		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	être transmis par différents moyens, notamment en accédant au Web, via un courrier électronique, dans les pièces jointes d'un courrier électronique et par des périphériques de stockage portables . Les insertions de code malveillant sont possibles en raison de la présence de vulnérabilités dans le système d'information. Les mécanismes de protection contre les codes malveillants incluent, par exemple, les signatures antivirus et les technologies basées sur la réputation des sites. Diverses technologies et méthodes existent pour atténuer ou éliminer les répercussions des codes malveillants. Pour empêcher l'exécution du code non autorisé, il peut être efficace		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de mettre en place une gestion plus approfondie de la configuration et des contrôles complets de l'intégrité logicielle. Outre les off-the-shelf logiciels commercia ux, du code malveilla nt peut également être présent dans des logiciels conçus sur mesure. Cela peut inclure, entre autres, des bombes logiques, des portes dérobées et d'autres types de cyberattaques susceptibles d'affecte r les missions/ fonctions de l'entrepr ise. Les mécanisme s traditionnels de protection contre les codes malveilla nts ne peuvent pas toujours détecter ce type de code. Dans ce cas, les entreprises s'appuien t plutôt sur d'autres mesures de protectio n, notamment des pratiques de codage		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées, la gestion et le contrôle de la configuration, des processus d'approvi sionnement fiables et des pratiques de surveillance pour garantir que les logiciels n'exécute nt pas de fonctions autres que celles prévues. Les entrepris es peuvent justifier différentes actions en réponse à la détection d'un code malveilla nt. Par exemple, elles peuvent définir des actions en réponse à la détection d'un code malveillant lors d'analyses périodiqu es, en réponse à la détection de télécharg ements malveillants, et/ou en réponse à la détection d'un code malveillant lors d'une tentative d'ouvertu re ou d'exécution de fichiers. Contrôles associés : CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7,		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	SC-26, SC-44, SI-2, SI-4, SI-7. Références : NIST Special Publication 800-83.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3	L'organisation : a. Utilise des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie du système d'information pour détecter et éradiquer les codes malveillants ; b. Met à jour les mécanismes de protection contre les codes malveillants dès que de nouvelles versions sont disponibles conformément aux politiques et procédures de gestion de la configuration de l'entreprise ; c. Configure les mécanismes de protection contre les codes malveillants pour : 1. Effectuer des analyses périodiques du système d'information [Attribution : fréquence définie par l'organisation] et des analyses en temps	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	réel des fichiers provenant de sources externes sur [Sélection (un ou plusieurs) ; point de terminaison ; points d'entrée/sortie du réseau] lorsque les fichiers sont téléchargés, ouverts ou exécutés conformément à la politique de sécurité de l'entreprise ; et 2. [Sélection (un ou plusieurs) : Bloquer le code malveillant ; Mettre le code malveillant en quarantaine ; Envoyer une alerte à l'administrateur ; [Attribution : action définie par l'organisation]] après la détection d'un code malveillant ; et d. Répond aux faux positifs lors de la détection et de l'éradication des codes malveillants et à l'impact potentiel qui en résulte sur la disponibilité du système d'information. Conseils		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : les points d'entrée et de sortie des systèmes d'information incluent, par exemple, les pare-feu, les serveurs de messagerie électronique, les serveurs Web, les serveurs proxy, les serveurs d'accès à distance, les stations de travail, les ordinateurs portables et les appareils mobiles. Les codes malveillants comprennent notamment les virus, les vers, les chevaux de Troie et les logiciels espions. Le code malveillant peut également être codé dans différents formats (par exemple, UUENCODE, Unicode), contenu dans des fichiers compressés ou masqués, ou masqué dans des fichiers à l'aide de la stéganographie. Les codes malveillants peuvent		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	être transmis par différents moyens, notamment en accédant au Web, via un courrier électronique, dans les pièces jointes d'un courrier électronique et par des périphériques de stockage portables . Les insertions de code malveillant sont possibles en raison de la présence de vulnérabilités dans le système d'information. Les mécanismes de protection contre les codes malveillants incluent, par exemple, les signatures antivirus et les technologies basées sur la réputation des sites. Diverses technologies et méthodes existent pour atténuer ou éliminer les répercussions des codes malveillants. Pour empêcher l'exécution du code non autorisé, il peut être efficace		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de mettre en place une gestion plus approfondie de la configuration et des contrôles complets de l'intégrité logicielle. Outre les off-the-shelf logiciels commercia ux, du code malveilla nt peut également être présent dans des logiciels conçus sur mesure. Cela peut inclure, entre autres, des bombes logiques, des portes dérobées et d'autres types de cyberattaques susceptibles d'affecte r les missions/ fonctions de l'entrepr ise. Les mécanisme s traditionnels de protection contre les codes malveilla nts ne peuvent pas toujours détecter ce type de code. Dans ce cas, les entreprises s'appuien t plutôt sur d'autres mesures de protectio n, notamment des pratiques de codage		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées, la gestion et le contrôle de la configuration, des processus d'approvi sionnement fiables et des pratiques de surveillance pour garantir que les logiciels n'exécute nt pas de fonctions autres que celles prévues. Les entrepris es peuvent justifier différentes actions en réponse à la détection d'un code malveilla nt. Par exemple, elles peuvent définir des actions en réponse à la détection d'un code malveillant lors d'analyses périodiqu es, en réponse à la détection de télécharg ements malveillants, et/ou en réponse à la détection d'un code malveillant lors d'une tentative d'ouvertu re ou d'exécution de fichiers. Contrôles associés : CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7,		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	SC-26, SC-44, SI-2, SI-4, SI-7. Références : NIST Special Publication 800-83.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3	L'organisation : a. Utilise des mécanismes de protection contre les codes malveillants aux points d'entrée et de sortie du système d'information pour détecter et éradiquer les codes malveillants ; b. Met à jour les mécanismes de protection contre les codes malveillants dès que de nouvelles versions sont disponibles conformément aux politiques et procédures de gestion de la configuration de l'entreprise ; c. Configure les mécanismes de protection contre les codes malveillants pour : 1. Effectuer des analyses périodiques du système d'information [Attribution : fréquence définie par l'organisation] et des analyses en temps	ecs-task-definition-memory-hard-limit	Limiter la mémoire maximale disponible sur vos conteneurs Amazon Elastic Container Service (ECS) garantit que vos ressources ne peuvent pas être utilisées de manière abusive en cas d'accès malveillant à vos conteneurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	réel des fichiers provenant de sources externes sur [Sélection (un ou plusieurs) ; point de terminaison ; points d'entrée/sortie du réseau] lorsque les fichiers sont téléchargés, ouverts ou exécutés conformément à la politique de sécurité de l'entreprise ; et 2. [Sélection (un ou plusieurs) : Bloquer le code malveillant ; Mettre le code malveillant en quarantaine ; Envoyer une alerte à l'administrateur ; [Attribution : action définie par l'organisation]] après la détection d'un code malveillant ; et d. Répond aux faux positifs lors de la détection et de l'éradication des codes malveillants et à l'impact potentiel qui en résulte sur la disponibilité du système d'information. Conseils		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	supplémentaires : les points d'entrée et de sortie des systèmes d'information incluent, par exemple, les pare-feu, les serveurs de messagerie électronique, les serveurs Web, les serveurs proxy, les serveurs d'accès à distance, les stations de travail, les ordinateurs portables et les appareils mobiles. Les codes malveillants comprennent notamment les virus, les vers, les chevaux de Troie et les logiciels espions. Le code malveillant peut également être codé dans différents formats (par exemple, UUENCODE, Unicode), contenu dans des fichiers compressés ou masqués, ou masqué dans des fichiers à l'aide de la stéganographie. Les codes malveillants peuvent		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	être transmis par différents moyens, notamment en accédant au Web, via un courrier électronique, dans les pièces jointes d'un courrier électronique et par des périphériques de stockage portables . Les insertions de code malveillant sont possibles en raison de la présence de vulnérabilités dans le système d'information. Les mécanismes de protection contre les codes malveillants incluent, par exemple, les signatures antivirus et les technologies basées sur la réputation des sites. Diverses technologies et méthodes existent pour atténuer ou éliminer les répercussions des codes malveillants. Pour empêcher l'exécution du code non autorisé, il peut être efficace		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de mettre en place une gestion plus approfondie de la configuration et des contrôles complets de l'intégrité logicielle. Outre les off-the-shelf logiciels commercia ux, du code malveilla nt peut également être présent dans des logiciels conçus sur mesure. Cela peut inclure, entre autres, des bombes logiques, des portes dérobées et d'autres types de cyberattaques susceptibles d'affecte r les missions/ fonctions de l'entrepr ise. Les mécanisme s traditionnels de protection contre les codes malveilla nts ne peuvent pas toujours détecter ce type de code. Dans ce cas, les entreprises s'appuien t plutôt sur d'autres mesures de protectio n, notamment des pratiques de codage		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées, la gestion et le contrôle de la configuration, des processus d'approvi sionnement fiables et des pratiques de surveillance pour garantir que les logiciels n'exécute nt pas de fonctions autres que celles prévues. Les entrepris es peuvent justifier différentes actions en réponse à la détection d'un code malveilla nt. Par exemple, elles peuvent définir des actions en réponse à la détection d'un code malveillant lors d'analyses périodiqu es, en réponse à la détection de télécharg ements malveillants, et/ou en réponse à la détection d'un code malveillant lors d'une tentative d'ouvertu re ou d'exécution de fichiers. Contrôles associés : CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7,		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	SC-26, SC-44, SI-2, SI-4, SI-7. Références : NIST Special Publication 800-83.		
SI-4(1)	L'organisation connecte et configure des outils individuels de détection d'intrusion dans un système de détection d'intrusion à l'échelle du système d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(2)	L'organisation utilise des outils automatisés pour analyser les événements en temps quasi réel.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(2)	L'organisation utilise des outils automatisés pour analyser les événements en temps quasi réel.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(2)	L'organisation utilise des outils automatisés pour analyser les événements en temps quasi réel.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(4)	Le système d'information surveille constamment le trafic de communications entrant et sortant pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(4)	Le système d'information surveille constamment le trafic de communications entrant et sortant pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(4)	Le système d'information surveille constamment le trafic de communications entrant et sortant pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(4)	Le système d'information surveille constamment le trafic de communications entrant et sortant pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	wafv2-logging-enab led	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	L'organisation : a. Reçoit des alertes, des conseils et des directives de sécurité du système d'information de la part de [Attribution : organisations externes définies par l'organisation] sur une base continue ; b. Génère des alertes, des conseils et des directives de sécurité internes si nécessaire ; c. Diffuse des alertes, des conseils et des directives de sécurité à : [Sélection (un ou plusieurs) : [Attribution : personnel ou rôles définis par l'organisation] ; [Attribution : éléments définis par l'organisation dans l'organisation] ; [Attribution : organisations externes définies par l'organisation] ; et d. Applique les directives de sécurité conformément aux délais prédéfinis ou	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informe l'organisme émetteur du degré de non-conformité. Conseils supplémentaires : l'équipe United States Computer Emergency Readiness(US-CERT) génère des alertes et des conseils de sécurité afin d'assurer une connaissance de la situation au sein du gouvernement fédéral. Les directives de sécurité sont émises par l'OMB ou par d'autres organisations désignées ayant la responsabilité et le pouvoir d'émettre de telles directives. Se conformer aux directives de sécurité est essentiel le en raison de l'aspect critique de bon nombre de ces directives et des effets négatifs immédiats potentiels sur les opérations et les ressources de l'organisation,		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les individus, les autres organisat ions et le pays si les directives ne sont pas mises en œuvre en temps opportun. Les organisations externes incluent, par exemple, les partenair es commerciaux/de missions externes, les partenaires de la chaîne d'approvi sionnement, les fournisseurs de services externes et d'autres organisat ions similaires ou soutenant le projet. Contrôle associé : SI-2. Références : NIST Special Publicati on 800-40.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	L'organisation : a. Reçoit des alertes, des conseils et des directives de sécurité du système d'informa tion de la part de [Attribution : organisat ions externes définies par l'organisation] sur une base continue ; b. Génère des alertes, des conseils et des directives de sécurité internes si nécessair e ; c. Diffuse des alertes, des conseils et des directives de sécurité à : [Sélectio n (un ou plusieurs) : [Attribution : personnel ou rôles définis par l'organis ation] ; [Attribution : éléments définis par l'organisation dans l'organisation] ; [Attribution : organisat ions externes définies par l'organisation] ; et d. Applique les directives de sécurité conformément aux délais prédéfinis ou	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informe l'organis me émetteur du degré de non-confo rmité. Conseils supplémentaires : l'équipe United States Computer Emergency Readiness(US-CERT) génère des alertes et des conseils de sécurité afin d'assurer une connaissance de la situation au sein du gouvernement fédéral. Les directive s de sécurité sont émises par l'OMB ou par d'autres organisat ions désignées ayant la responsabilité et le pouvoir d'émettre de telles directive s. Se conformer aux directives de sécurité est essentiel le en raison de l'aspect critique de bon nombre de ces directives et des effets négatifs immédiats potentiel s sur les opération s et les ressource s de l'organisation,		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les individus, les autres organisat ions et le pays si les directives ne sont pas mises en œuvre en temps opportun. Les organisations externes incluent, par exemple, les partenair es commerciaux/de missions externes, les partenaires de la chaîne d'approvi sionnement, les fournisseurs de services externes et d'autres organisat ions similaires ou soutenant le projet. Contrôle associé : SI-2. Références : NIST Special Publicati on 800-40.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	L'organisation : a. Reçoit des alertes, des conseils et des directives de sécurité du système d'information de la part de [Attribution : organisations externes définies par l'organisation] sur une base continue ; b. Génère des alertes, des conseils et des directives de sécurité internes si nécessaire ; c. Diffuse des alertes, des conseils et des directives de sécurité à : [Sélection (un ou plusieurs) : [Attribution : personnel ou rôles définis par l'organisation] ; [Attribution : éléments définis par l'organisation dans l'organisation] ; [Attribution : organisations externes définies par l'organisation] ; et d. Applique les directives de sécurité conformément aux délais prédéfinis ou	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informe l'organis me émetteur du degré de non-confo rmité. Conseils supplémentaires : l'équipe United States Computer Emergency Readiness(US-CERT) génère des alertes et des conseils de sécurité afin d'assurer une connaissance de la situation au sein du gouvernement fédéral. Les directive s de sécurité sont émises par l'OMB ou par d'autres organisat ions désignées ayant la responsabilité et le pouvoir d'émettre de telles directive s. Se conformer aux directives de sécurité est essentiel le en raison de l'aspect critique de bon nombre de ces directives et des effets négatifs immédiats potentiel s sur les opération s et les ressource s de l'organisation,		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les individus, les autres organisat ions et le pays si les directives ne sont pas mises en œuvre en temps opportun. Les organisations externes incluent, par exemple, les partenair es commerciaux/de missions externes, les partenaires de la chaîne d'approvi sionnement, les fournisseurs de services externes et d'autres organisat ions similaires ou soutenant le projet. Contrôle associé : SI-2. Références : NIST Special Publicati on 800-40.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-5	L'organisation : a. Reçoit des alertes, des conseils et des directives de sécurité du système d'informa tion de la part de [Attribution : organisat ions externes définies par l'organisation] sur une base continue ; b. Génère des alertes, des conseils et des directives de sécurité internes si nécessair e ; c. Diffuse des alertes, des conseils et des directives de sécurité à : [Sélectio n (un ou plusieurs) : [Attribution : personnel ou rôles définis par l'organis ation] ; [Attribution : éléments définis par l'organisation dans l'organisation] ; [Attribution : organisat ions externes définies par l'organisation] ; et d. Applique les directives de sécurité conformément aux délais prédéfinis ou	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	informe l'organis me émetteur du degré de non-confo rmité. Conseils supplémentaires : l'équipe United States Computer Emergency Readiness(US-CERT) génère des alertes et des conseils de sécurité afin d'assurer une connaissance de la situation au sein du gouvernement fédéral. Les directive s de sécurité sont émises par l'OMB ou par d'autres organisat ions désignées ayant la responsabilité et le pouvoir d'émettre de telles directive s. Se conformer aux directives de sécurité est essentiel le en raison de l'aspect critique de bon nombre de ces directives et des effets négatifs immédiats potentiel s sur les opération s et les ressource s de l'organisation,		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les individus, les autres organisat ions et le pays si les directives ne sont pas mises en œuvre en temps opportun. Les organisations externes incluent, par exemple, les partenair es commerciaux/de missions externes, les partenaires de la chaîne d'approvi sionnement, les fournisseurs de services externes et d'autres organisat ions similaires ou soutenant le projet. Contrôle associé : SI-2. Références : NIST Special Publicati on 800-40.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7(1)	Le système d'information contrôle l'intégrité des événements de sécurité au moins une fois par mois.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7(1)	Le système d'information contrôle l'intégrité des événements de sécurité au moins une fois par mois.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7(1)	Le système d'information contrôle l'intégrité des événements de sécurité au moins une fois par mois.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7	L'organisation utilise des outils d'audit de l'intégrité pour détecter les modifications non autorisées des [Attribution : logiciels, microprogrammes et informations définis par l'organisation].	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-11	Le système d'information : a. Génère des messages d'erreur qui fournissent les informations nécessaires pour prendre des mesures correctives sans révéler d'informations susceptibles d'être exploitées par des adversaires ; et b. Affiche les messages d'erreur uniquement à [Attribution : personnel ou rôles définis par l'organisation]. Conseils supplémentaires : les organisations examinent attentivement la structure /le contenu des messages d'erreur. Le degré de capacité des systèmes d'information à identifier et gérer les situations d'erreur dépend de la politique de l'entreprise et des exigences opérationnelles. Les informations susceptib	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les d'être exploitées par des adversaires incluent, par exemple, des tentatives de connexion erronées avec des mots de passe saisis par erreur dans le champ dédié au nom d'utilisa teur, des informati ons sur la mission/l 'entreprise pouvant provenir (si elles n'ont pas été explicitement publiées) d'informa tions enregistrées, et des informations personnelles telles que les numéros de compte, les numéros de sécurité sociale et les numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de canal secret pour la transmiss ion d'informations. Contrôles associés : AU-2, AU-3, SC-31. Amélioration des contrôles : aucune. Références : aucune.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-11	Le système d'information : a. Génère des messages d'erreur qui fournissent les informations nécessaires pour prendre des mesures correctives sans révéler d'informations susceptibles d'être exploitées par des adversaires ; et b. Affiche les messages d'erreur uniquement à [Attribution : personnel ou rôles définis par l'organisation]. Conseils supplémentaires : les organisations examinent attentivement la structure /le contenu des messages d'erreur. Le degré de capacité des systèmes d'information à identifier et gérer les situations d'erreur dépend de la politique de l'entreprise et des exigences opérationnelles. Les informations susceptib	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les d'être exploitées par des adversaires incluent, par exemple, des tentatives de connexion erronées avec des mots de passe saisis par erreur dans le champ dédié au nom d'utilisa teur, des informati ons sur la mission/l 'entreprise pouvant provenir (si elles n'ont pas été explicitement publiées) d'informa tions enregistrées, et des informations personnelles telles que les numéros de compte, les numéros de sécurité sociale et les numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de canal secret pour la transmiss ion d'informations. Contrôles associés : AU-2, AU-3, SC-31. Amélioration des contrôles : aucune. Références : aucune.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-11	Le système d'information : a. Génère des messages d'erreur qui fournissent les informations nécessaires pour prendre des mesures correctives sans révéler d'informations susceptibles d'être exploitées par des adversaires ; et b. Affiche les messages d'erreur uniquement à [Attribution : personnel ou rôles définis par l'organisation]. Conseils supplémentaires : les organisations examinent attentivement la structure /le contenu des messages d'erreur. Le degré de capacité des systèmes d'information à identifier et gérer les situations d'erreur dépend de la politique de l'entreprise et des exigences opérationnelles. Les informations susceptib	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les d'être exploitées par des adversaires incluent, par exemple, des tentatives de connexion erronées avec des mots de passe saisis par erreur dans le champ dédié au nom d'utilisa teur, des informati ons sur la mission/l 'entreprise pouvant provenir (si elles n'ont pas été explicitement publiées) d'informa tions enregistrées, et des informations personnelles telles que les numéros de compte, les numéros de sécurité sociale et les numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de canal secret pour la transmiss ion d'informations. Contrôles associés : AU-2, AU-3, SC-31. Amélioration des contrôles : aucune. Références : aucune.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-11	Le système d'information : a. Génère des messages d'erreur qui fournissent les informations nécessaires pour prendre des mesures correctives sans révéler d'informations susceptibles d'être exploitées par des adversaires ; et b. Affiche les messages d'erreur uniquement à [Attribution : personnel ou rôles définis par l'organisation]. Conseils supplémentaires : les organisations examinent attentivement la structure /le contenu des messages d'erreur. Le degré de capacité des systèmes d'information à identifier et gérer les situations d'erreur dépend de la politique de l'entreprise et des exigences opérationnelles. Les informations susceptib	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les d'être exploitées par des adversaires incluent, par exemple, des tentatives de connexion erronées avec des mots de passe saisis par erreur dans le champ dédié au nom d'utilisa teur, des informati ons sur la mission/l 'entreprise pouvant provenir (si elles n'ont pas été explicitement publiées) d'informa tions enregistrées, et des informations personnelles telles que les numéros de compte, les numéros de sécurité sociale et les numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de canal secret pour la transmiss ion d'informations. Contrôles associés : AU-2, AU-3, SC-31. Amélioration des contrôles : aucune. Références : aucune.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-11	Le système d'information : a. Génère des messages d'erreur qui fournissent les informations nécessaires pour prendre des mesures correctives sans révéler d'informations susceptibles d'être exploitées par des adversaires ; et b. Affiche les messages d'erreur uniquement à [Attribution : personnel ou rôles définis par l'organisation]. Conseils supplémentaires : les organisations examinent attentivement la structure /le contenu des messages d'erreur. Le degré de capacité des systèmes d'information à identifier et gérer les situations d'erreur dépend de la politique de l'entreprise et des exigences opérationnelles. Les informations susceptib	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les d'être exploitées par des adversaires incluent, par exemple, des tentatives de connexion erronées avec des mots de passe saisis par erreur dans le champ dédié au nom d'utilisa teur, des informati ons sur la mission/l 'entreprise pouvant provenir (si elles n'ont pas été explicitement publiées) d'informa tions enregistrées, et des informations personnelles telles que les numéros de compte, les numéros de sécurité sociale et les numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de canal secret pour la transmiss ion d'informations. Contrôles associés : AU-2, AU-3, SC-31. Amélioration des contrôles : aucune. Références : aucune.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-11	Le système d'information : a. Génère des messages d'erreur qui fournissent les informations nécessaires pour prendre des mesures correctives sans révéler d'informations susceptibles d'être exploitées par des adversaires ; et b. Affiche les messages d'erreur uniquement à [Attribution : personnel ou rôles définis par l'organisation]. Conseils supplémentaires : les organisations examinent attentivement la structure /le contenu des messages d'erreur. Le degré de capacité des systèmes d'information à identifier et gérer les situations d'erreur dépend de la politique de l'entreprise et des exigences opérationnelles. Les informations susceptib	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les d'être exploitées par des adversaires incluent, par exemple, des tentatives de connexion erronées avec des mots de passe saisis par erreur dans le champ dédié au nom d'utilisa teur, des informati ons sur la mission/l 'entreprise pouvant provenir (si elles n'ont pas été explicitement publiées) d'informa tions enregistrées, et des informations personnelles telles que les numéros de compte, les numéros de sécurité sociale et les numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de canal secret pour la transmiss ion d'informations. Contrôles associés : AU-2, AU-3, SC-31. Amélioration des contrôles : aucune. Références : aucune.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-11	Le système d'information : a. Génère des messages d'erreur qui fournissent les informations nécessaires pour prendre des mesures correctives sans révéler d'informations susceptibles d'être exploitées par des adversaires ; et b. Affiche les messages d'erreur uniquement à [Attribution : personnel ou rôles définis par l'organisation]. Conseils supplémentaires : les organisations examinent attentivement la structure /le contenu des messages d'erreur. Le degré de capacité des systèmes d'information à identifier et gérer les situations d'erreur dépend de la politique de l'entreprise et des exigences opérationnelles. Les informations susceptib	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	les d'être exploitées par des adversaires incluent, par exemple, des tentatives de connexion erronées avec des mots de passe saisis par erreur dans le champ dédié au nom d'utilisa teur, des informati ons sur la mission/l 'entreprise pouvant provenir (si elles n'ont pas été explicitement publiées) d'informa tions enregistrées, et des informations personnelles telles que les numéros de compte, les numéros de sécurité sociale et les numéros de carte de crédit. En outre, les messages d'erreur peuvent servir de canal secret pour la transmiss ion d'informations. Contrôles associés : AU-2, AU-3, SC-31. Amélioration des contrôles : aucune. Références : aucune.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-16	Le système d'information applique [Attribution : mesures de sécurité définies par l'organisation] pour protéger son stockage de toute exécution de code non autorisée. Conseils supplémentaires : certains adversaires lancent des attaques dans le but d'exécuter un code dans des zones de mémoire non exécutables ou dans des emplacements de stockage interdits d'accès. Les mesures de sécurité utilisées pour protéger le stockage impliquent notamment de prévenir l'exécution des données et d'effectuer une aléatorisation de la disposition des espaces dédiés aux adresses. Les mesures prévenant l'exécution des données peuvent	ecs-task-definition-memory-hard-limit	Limiter la mémoire maximale disponible sur vos conteneurs Amazon Elastic Container Service (ECS) garantit que vos ressources ne peuvent pas être utilisées de manière abusive en cas d'accès malveillant à vos conteneurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	être appliquées via le matériel ou le logiciel, le matériel rendant le mécanisme encore plus puissant. Contrôles associés : AC-25, SC-3. Amélioration des contrôles : aucune. Références : aucune.		

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for FedRAMP (Moderate).

Bonnes pratiques de fonctionnement pour FFIEC

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les domaines de l'outil d'évaluation de la cybersécurité du Federal Financial Institutions Examination Council (FFIEC) et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles de l'outil d'évaluation de la cybersécurité FFIEC. Le contrôle des outils d'évaluation de la cybersécurité du FFIEC peut être lié à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.G.IT.B.1	Un inventaire des actifs organisationnels (par exemple, le matériel, les logiciels , les données et les systèmes hébergés en externe) est tenu à jour.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
D1.G.IT.B.1	Un inventaire des actifs organisationnels (par exemple, le matériel, les logiciels , les données et les systèmes hébergés	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2)

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	en externe) est tenu à jour.		en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
D1.G.IT.B.1	Un inventaire des actifs organisationnels (par exemple, le matériel, les logiciels, les données et les systèmes hébergés en externe) est tenu à jour.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.G.IT.B.1	Un inventaire des actifs organisationnels (par exemple, le matériel, les logiciels , les données et les systèmes hébergés en externe) est tenu à jour.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.Rm.B.1	L'établissement possède une ou plusieurs fonctions de gestion des risques liés à la sécurité de l'information et à la continuité des activités.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.RM.RA.B.2	L'évaluation des risques identifie les systèmes basés sur Internet et les transactions à haut risque qui justifient des contrôles d'authentification supplémentaires.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
D1.RM.RA.B.2	L'évaluation des risques identifie les systèmes basés sur Internet et les transactions à haut risque qui justifient des contrôles d'authentification supplémentaires.	annual-risk-assessment-performed (vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.TC.Tr.B.2	La formation annuelle sur la sécurité des informations porte sur la réponse aux incidents, les cybermena ces actuelles (par exemple, le phishing, le spear phishing, l'ingénierie sociale et la sécurité mobile) et les problèmes émergents.	security-awareness -program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.IS.Is.B.1	Les menaces relatives à la sécurité des informations sont collectées et partagées avec les employés concernés en interne.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.IS.Is.B.1	Les menaces relatives à la sécurité des informations sont collectées et partagées avec les employés concernés en interne.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.IS.Is.B.1	Les menaces relatives à la sécurité des informations sont collectées et partagées avec les employés concernés en interne.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
D2.MA.Ma.B.1	Les enregistrements des journaux d'audit et d'autres journaux d'événements de sécurité sont analysés et conservés de manière sécurisée.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.MA.Ma.B.2	Les journaux d'événements informatiques sont utilisés pour les enquêtes après la survenue d'un événement.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.TI.Ti.B.1	L'institution appartient ou est abonnée à une ou plusieurs sources de partage d'informations sur les menaces et les vulnérabilités qui fournissent des informations sur les menaces (par exemple, FS-ISAC, US-CERT).	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.TI.Ti.B.1	L'institution appartient ou est abonnée à une ou plusieurs sources de partage d'informations sur les menaces et les vulnérabilités qui fournissent des informations sur les menaces (par exemple, FS-ISAC, US-CERT).	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.TI.Ti.B.2	Les informations sur les menaces sont utilisées pour surveiller les éventuelles menaces et vulnérabilités.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.TI.Ti.B.2	Les informations sur les menaces sont utilisées pour surveiller les éventuelles menaces et vulnérabilités.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.TI.Ti.B.2	Les informations sur les menaces sont utilisées pour surveiller les éventuelles menaces et vulnérabilités.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.TI.Ti.B.3	Les informations sur les menaces sont utilisées pour améliorer la gestion et les contrôles des risques internes.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D2.TI.Ti.B.3	Les informations sur les menaces sont utilisées pour améliorer la gestion et les contrôles des risques internes.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.1	Un programme de gestion des correctifs est mis en œuvre et garantit que les correctifs logiciels et micrologiciels sont appliqués en temps opportun.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.1	Un programme de gestion des correctif s est mis en œuvre et garantit que les correctifs logiciels et micrologiciels sont appliqués en temps opportun.	elastic-beanstalk-managed-updates-en abled	L'activation des mises à jour de plateforme gérées pour un environne ment Amazon Elastic Beanstalk garantit l'installation des derniers correctif s, mises à jour et fonctionnalités de la plateforme disponibl es pour l'environ nement. La sécurisat ion des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.1	Un programme de gestion des correctifs est mis en œuvre et garantit que les correctifs logiciels et micrologiciels sont appliqués en temps opportun.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.1	Un programme de gestion des correctifs est mis en œuvre et garantit que les correctifs logiciels et micrologiciels sont appliqués en temps opportun.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.3	Les rapports de gestion des correctifs sont analysés et signalent les correctifs de sécurité manquants.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.3	Les rapports de gestion des correctif s sont analysés et signalent les correctifs de sécurité manquants.	elastic-beanstalk-managed-updates-en abled	L'activation des mises à jour de plateforme gérées pour un environne ment Amazon Elastic Beanstalk garantit l'installation des derniers correctif s, mises à jour et fonctionnalités de la plateforme disponibl es pour l'environ nement. La sécurisat ion des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.3	Les rapports de gestion des correctifs sont analysés et signalent les correctifs de sécurité manquants.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.CC.PM.B.3	Les rapports de gestion des correctifs sont analysés et signalent les correctifs de sécurité manquants.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.1	L'établissement peut détecter les activités anormales grâce à une surveillance effectuée sur l'ensemble de l'environnement.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.1	L'établissement peut détecter les activités anormales grâce à une surveillance effectuée sur l'ensemble de l'environnement.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.1	L'établissement peut détecter les activités anormales grâce à une surveillance effectuée sur l'ensemble de l'environnement.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.2	Les transactions clients générant des alertes d'activit é anormale sont surveillées et analysées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.2	Les transactions clients générant des alertes d'activité anormale sont surveillées et analysées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
D3.DC.An.B.3	Les journaux d'accès physiques et/ou logiques sont analysés en cas d'événement détecté.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.3	Les journaux d'accès physiques et/ ou logiques sont analysés en cas d'événement détecté.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.4	L'accès aux systèmes critiques par des tiers est surveillé afin de détecter toute activité non autorisée ou inhabituelle	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.5	Les privilèges élevés accordés aux utilisateurs sont surveillés.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.An.B.5	Les privilèges élevés accordés aux utilisate urs sont surveillés.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.1	Une référence est établie pour définir l'activité normale du réseau.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.2	Des mécanismes (par exemple, alertes antivirus, alertes d'événements liés aux journaux) sont en place pour alerter la direction en cas d'attaques potentiel les.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.3	Des processus sont utilisés pour surveiller la présence d'utilisateurs, d'appareils, de connexions et de logiciels non autorisés.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.3	Des processus sont utilisés pour surveiller la présence d'utilisateurs, d'appareils, de connexions et de logiciels non autorisés.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.3	Des processus sont utilisés pour surveiller la présence d'utilisateurs, d'appareils, de connexions et de logiciels non autorisés.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Ev.B.3	Des processus sont utilisés pour surveiller la présence d'utilisateurs, d'appareils, de connexions et de logiciels non autorisés.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Th.B.1	Des tests indépendants (y compris des tests de pénétration et des analyses de vulnérabilité) sont effectués conformément à l'évaluation des risques des systèmes externes et du réseau interne.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Th.B.1	Des tests indépendants (y compris des tests de pénétration et des analyses de vulnérabilité) sont effectués conformément à l'évaluation des risques des systèmes externes et du réseau interne.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.DC.Th.B.1	Des tests indépendants (y compris des tests de pénétration et des analyses de vulnérabilité) sont effectués conformément à l'évaluation des risques des systèmes externes et du réseau interne.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confidentielles est accordé selon leurs responsabilités professionnelles et le principe du moindre privilège.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confidentielles est accordé selon leurs responsabilités professionnelles et le principe du moindre privilège.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confident ielles est accordé selon leurs responsab ilités professionnelles et le principe du moindre privilège.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
D3.PC.Am.B.1	L'accès des employés aux systèmes et aux données confidentielles est accordé selon leurs responsabilités professionnelles et le principe du moindre privilège.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.10	Les environnements de production sont séparés des autres événements afin d'empêcher tout accès non autorisé ou toute modification des actifs d'informa tion. (* S/O s'il n'existe aucun environne ment de production dans l'établissement ou chez la partie prenante tierce de l'établissement.)	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
D3.PC.Am.B.10	Les environnements de production sont séparés des autres événements afin d'empêcher tout accès non autorisé ou toute modification des actifs d'informa tion. (* S/O s'il n'existe aucun environne ment de production dans l'établissement ou chez la partie prenante tierce de l'établissement.)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.10	Les environnements de production sont séparés des autres événements afin d'empêcher tout accès non autorisé ou toute modification des actifs d'informa tion. (* S/O s'il n'existe aucun environne ment de production dans l'établissement ou chez la partie prenante tierce de l'établissement.)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.10	Les environnements de production sont séparés des autres événements afin d'empêcher tout accès non autorisé ou toute modification des actifs d'informa tion. (* S/O s'il n'existe aucun environne ment de production dans l'établissement ou chez la partie prenante tierce de l'établissement.)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informati ons administratives sur chaque principal.
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	backup-recovery-po int-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
D3.PC.Am.B.12	Tous les mots de passe sont chiffrés pendant le stockage et quand ils sont en transit.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.13	Les données confidentielles sont cryptées lorsqu'el les sont transmise s sur des réseaux publics ou non fiables (Internet, par exemple).	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
D3.PC.Am.B.13	Les données confidentielles sont cryptées lorsqu'el les sont transmise s sur des réseaux publics ou non fiables (Internet, par exemple).	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.13	Les données confidentielles sont cryptées lorsqu'el les sont transmise s sur des réseaux publics ou non fiables (Internet, par exemple).	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
D3.PC.Am.B.13	Les données confidentielles sont cryptées lorsqu'el les sont transmise s sur des réseaux publics ou non fiables (Internet, par exemple).	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.13	Les données confidentielles sont cryptées lorsqu'elles sont transmises sur des réseaux publics ou non fiables (Internet, par exemple).	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
D3.PC.Am.B.13	Les données confidentielles sont cryptées lorsqu'elles sont transmises sur des réseaux publics ou non fiables (Internet, par exemple).	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.13	Les données confidentielles sont cryptées lorsqu'elles sont transmises sur des réseaux publics ou non fiables (Internet, par exemple).	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.15	L'accès à distance aux systèmes critiques par les employés, les sous-traitants et les tiers s'effectue via des connexions chiffrées et une authentification multifactorielle.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.15	L'accès à distance aux systèmes critiques par les employés, les sous-traitants et les tiers s'effectue via des connexions chiffrées et une authentification multifactorielle.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.15	L'accès à distance aux systèmes critiques par les employés, les sous-traitants et les tiers s'effectue via des connexions chiffrées et une authentification multifactorielle.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.15	L'accès à distance aux systèmes critiques par les employés, les sous-traitants et les tiers s'effectue via des connexions chiffrées et une authentification multifactorielle.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.15	L'accès à distance aux systèmes critiques par les employés, les sous-traitants et les tiers s'effectue via des connexions chiffrées et une authentification multifactorielle.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
D3.PC.Am.B.15	L'accès à distance aux systèmes critiques par les employés, les sous-traitants et les tiers s'effectue via des connexions chiffrées et une authentification multifactorielle.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.15	L'accès à distance aux systèmes critiques par les employés, les sous-traitants et les tiers s'effectue via des connexions chiffrées et une authentification multifactorielle.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.16	Des contrôles administratifs, physiques ou techniques ont été mis en place pour empêcher les utilisateurs sans responsabilités administratives d'installer des logiciels non autorisés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.16	Des contrôles administratifs, physiques ou techniques ont été mis en place pour empêcher les utilisateurs sans responsabilités administratives d'installer des logiciels non autorisés.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.16	Des contrôles administratifs, physiques ou techniques ont été mis en place pour empêcher les utilisateurs sans responsabilités administratives d'installer des logiciels non autorisés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.16	Des contrôles administratifs, physiques ou techniques ont été mis en place pour empêcher les utilisateurs sans responsabilités administratives d'installer des logiciels non autorisés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.2	L'accès des employés aux systèmes et aux données confidentielles assure la séparation des tâches.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.2	L'accès des employés aux systèmes et aux données confident ielles assure la séparation des tâches.	iam-user-group-membership-check	AWS Identity and Access Managemen t (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisate urs plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.2	L'accès des employés aux systèmes et aux données confident ielles assure la séparation des tâches.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.3	Les privilèges élevés (par exemple, les privilèges d'administrateur) sont limités et étroitement contrôlés (par exemple, ils sont attribués à des individus, ne sont pas partagés, et nécessitent des contrôles de mot de passe renforcés)	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.3	Les privilèges élevés (par exemple, les privilèges d'administrateur) sont limités et étroitement contrôlés (par exemple, ils sont attribués à des individus, ne sont pas partagés, et nécessitent des contrôles de mot de passe renforcés)	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.3	Les privilèges élevés (par exemple, les privilèges d'administrateur) sont limités et étroitement contrôlés (par exemple, ils sont attribués à des individus, ne sont pas partagés, et nécessitent des contrôles de mot de passe renforcés).	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.3	Les privilèges élevés (par exemple, les privilèges d'adminis trateur) sont limités et étroitement contrôlés (par exemple, ils sont attribués à des individus, ne sont pas partagés, et nécessite nt des contrôles de mot de passe renforcés)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.3	Les privilèges élevés (par exemple, les privilèges d'administrateur) sont limités et étroitement contrôlés (par exemple, ils sont attribués à des individus, ne sont pas partagés, et nécessitent des contrôles de mot de passe renforcés)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.3	Les privilèges élevés (par exemple, les privilèges d'administrateur) sont limités et étroitement contrôlés (par exemple, ils sont attribués à des individus, ne sont pas partagés, et nécessitent des contrôles de mot de passe renforcés)	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
D3.PC.Am.B.6	Pour accéder aux systèmes, aux applications et au matériel, une identification et une authentification réglementées sont requises.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.7	Les contrôles d'accès incluent des mots de passe complexes, ainsi que des tentatives de connexion et une réutilisation des mots de passe limitées.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Am.B.8	Tous les mots de passe par défaut et les comptes inutilisés par défaut sont modifiés avant la mise en œuvre du système.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.1	Des outils de défense du périmètre réseau (par exemple, routeur frontalier et pare-feu) sont utilisés.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.2	Les systèmes accessibles depuis Internet ou par des tiers sont protégés par des pare-feu ou d'autres dispositifs similaires.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.2	Les systèmes accessibles depuis Internet ou par des tiers sont protégés par des pare-feu ou d'autres dispositifs similaires.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.2	Les systèmes accessibles depuis Internet ou par des tiers sont protégés par des pare-feu ou d'autres dispositifs similaires.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.2	Les systèmes accessibles depuis Internet ou par des tiers sont protégés par des pare-feu ou d'autres dispositifs similaires.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.2	Les systèmes accessibles depuis Internet ou par des tiers sont protégés par des pare-feu ou d'autres dispositifs similaires.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.2	Les systèmes accessibles depuis Internet ou par des tiers sont protégés par des pare-feu ou d'autres dispositifs similaires.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.3	Tous les ports sont surveillés.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.3	Tous les ports sont surveillés.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
D3.PC.IM.B.3	Tous les ports sont surveillés.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.3	Tous les ports sont surveillés.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.3	Tous les ports sont surveillés.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.3	Tous les ports sont surveillés.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.5	Les configurations des systèmes (pour les serveurs, les ordinateurs de bureau, les routeurs, etc.) respectent les normes du secteur et sont obligatoirement appliquées	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.5	Les configurations des systèmes (pour les serveurs, les ordinateurs de bureau, les routeurs, etc.) respectent les normes du secteur et sont obligatoirement appliquées	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.5	Les configurations des systèmes (pour les serveurs, les ordinateurs de bureau, les routeurs, etc.) respectent les normes du secteur et sont obligatoirement appliquées	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.6	Les ports, les fonctions, les protocoles et les services sont interdits s'ils ne sont plus nécessaires aux activités commercia les.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.6	Les ports, les fonctions, les protocoles et les services sont interdits s'ils ne sont plus nécessaires aux activités commercia les.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.6	Les ports, les fonctions, les protocoles et les services sont interdits s'ils ne sont plus nécessaires aux activités commercia les.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.IM.B.6	Les ports, les fonctions, les protocoles et les services sont interdits s'ils ne sont plus nécessaires aux activités commercia les.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.7	L'accès autorisant la modification des configurations des systèmes (y compris les machines virtuelles et les hyperviseurs) est contrôlé et surveillé.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.7	L'accès autorisant la modification des configurations des systèmes (y compris les machines virtuelles et les hyperviseurs) est contrôlé et surveillé.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.7	L'accès autorisant la modification des configurations des systèmes (y compris les machines virtuelles et les hypervisseurs) est contrôlé et surveillé.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.7	L'accès autorisant la modification des configurations des systèmes (y compris les machines virtuelles et les hyperviseurs) est contrôlé et surveillé.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.7	L'accès autorisant la modification des configurations des systèmes (y compris les machines virtuelles et les hypervisseurs) est contrôlé et surveillé.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Im.B.7	L'accès autorisant la modification des configurations des systèmes (y compris les machines virtuelles et les hyperviseurs) est contrôlé et surveillé.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
D3.PC.Im.B.7	L'accès autorisant la modification des configurations des systèmes (y compris les machines virtuelles et les hyperviseurs) est contrôlé et surveillé.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Se.B.1	Les développeurs travaillant pour l'établissement utilisent des pratiques de codage de programme sécurisées, dans le cadre du cycle de vie du développement du système (SDLC), conformes aux normes du secteur.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D3.PC.Se.B.1	Les développeurs travaillant pour l'établissement utilisent des pratiques de codage de programme sécurisées, dans le cadre du cycle de vie du développement du système (SDLC), conformes aux normes du secteur.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D4.C.Co.B.2	L'établissement vérifie que les connexions avec des tiers sont autorisées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D4.C.Co.B.2	L'établissement vérifie que les connexions avec des tiers sont autorisées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D4.C.Co.B.2	L'établissement vérifie que les connexions avec des tiers sont autorisées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D4.C.Co.B.2	L'établissement vérifie que les connexions avec des tiers sont autorisées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.1	Les paramètres d'alerte sont définis pour détecter les incidents de sécurité des informations qui entraînent des mesures d'atténuation des risques.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.1	Les paramètres d'alerte sont définis pour détecter les incidents de sécurité des informations qui entraînent des mesures d'atténuation des risques.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.1	Les paramètres d'alerte sont définis pour détecter les incidents de sécurité des informations qui entraînent des mesures d'atténuation des risques.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
D5.DR.De.B.2	Les rapports des performances du système contiennent des informations qui peuvent être utilisées comme indicateurs de risque pour détecter les incidents liés à la sécurité des informati ons	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.2	Les rapports des performances du système contiennent des informations qui peuvent être utilisées comme indicateurs de risque pour détecter les incidents liés à la sécurité des informations	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.DR.De.B.3	Des outils et des processus ont été mis en place pour détecter les incidents , émettre des alertes et déclencher le programme de réponse.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.ER.Es.B.4	Les incidents sont classés, enregistrés et suivis.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.
D5.IR.Pl.B.1	L'établissement a documenté la manière dont il réagira et répondra aux cyber incidents.	response-plan-exists-maintained (vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	rds-enhanced-monit oring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibi lité d'Amazon RDS. Vous disposez ainsi d'une visibilit é détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploieme nt multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegard e des données pour reprendre les opérations après un incident.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegarde des données pour reprendre les opérations après un incident.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegarde des données pour reprendre les opérations après un incident.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
D5.IR.PI.B.6	L'établissement prévoit d'utiliser des programmes liés à la continuité des activités, à la reprise après sinistre et à la sauvegarde des données pour reprendre les opérations après un incident.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for FFIEC.

Bonnes pratiques de fonctionnement pour Germany Cloud Computing Compliance Criteria Catalog (C5)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le catalogue allemand des critères de conformité du cloud computing (C5) et les règles de configuration AWS gérées. Chaque règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles C5 allemands. Un contrôle Germany C5 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
COS-01	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.
COS-01	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL

ID du contrôle	AWS Règle de configuration	Conseils
		Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
COS-01	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.
COS-01	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.
COS-01	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.

ID du contrôle	AWS Règle de configuration	Conseils
COS-01	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
COS-03	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
COS-03	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
COS-03	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
COS-03	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
COS-03	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
COS-03	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
COS-03	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
COS-03	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
COS-03	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
COS-03	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
COS-03	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
COS-05	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifact orielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
COS-05	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
COS-05	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
COS-05	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
COS-05	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
COS-05	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
COS-05	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
COS-05	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
COS-05	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
COS-05	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
COS-05	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
COS-05	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
COS-05	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
CRY-02	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-02	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-02	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classique s utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociati on SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociati on SSL assurent la compatibi lité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfini e pour vos écouteurs SSL. La politique de sécurité par défaut est : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politique s de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
CRY-02	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
CRY-02	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CRY-02	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-02	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CRY-02	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
CRY-02	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
CRY-03	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
CRY-03	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
CRY-03	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
CRY-03	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
CRY-03	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
CRY-03	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
CRY-03	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearc h Service.
CRY-03	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
CRY-03	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
CRY-03	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
CRY-03	s3-default-encryption-kms	Assurez-vous que le chiffreme nt est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartim ent Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
CRY-03	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-03	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
CRY-04	cmk-backing-key-rotation-en abled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.
DEV-07	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatc h pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
DEV-07	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.
DEV-07	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
DEV-07	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
DEV-07	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	access-keys-rotated	Les informations d'identif ication sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organis ation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
IDM-01	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
IDM-01	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
IDM-01	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
IDM-01	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.
IDM-01	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
IDM-01	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
IDM-01	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.
IDM-01	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
IDM-01	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	rds-instance-iam-authentication-enabled	Assurez-vous qu'une authentification AWS Identity and Access Management (IAM) est activée sur les instances Amazon Relational Database Service (Amazon RDS) afin de contrôler l'accès aux systèmes et aux actifs. Cela permet de chiffrer le trafic réseau à destination et en provenance de la base de données au moyen du protocole SSL. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-01	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommand é d'utiliser des politique s IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-03	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.
IDM-03	secretsmanager-secret-unuse d	Si des informations d'identif ication non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-08	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
CRY-01	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
IDM-09	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifact orielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-09	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
IDM-09	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
IDM-09	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
OPS-01	clb-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneur s et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.
OPS-01	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneur s et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-01	lambda-vpc-multi-az-check	Si votre fonction AWS Lambda est configurée pour se connecter à un cloud privé virtuel (VPC) dans votre compte, déployez la fonction AWS Lambda dans au moins deux zones de disponibi lité différentes afin de vous assurer que votre fonction est disponible pour traiter les événements en cas d'interru ption de service dans une seule zone.
OPS-01	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionn e sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-01	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-01	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
OPS-01	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-01	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-02	clb-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneur s et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.
OPS-02	autoscaling-group-elb-healt hcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-02	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modificat ions de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'applica tion. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifié s et d'identifier les causes possibles à étudier.
OPS-02	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneur s et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-02	lambda-vpc-multi-az-check	Si votre fonction AWS Lambda est configurée pour se connecter à un cloud privé virtuel (VPC) dans votre compte, déployez la fonction AWS Lambda dans au moins deux zones de disponibi lité différentes afin de vous assurer que votre fonction est disponible pour traiter les événements en cas d'interru ption de service dans une seule zone.
OPS-02	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionn e sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-02	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-02	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
OPS-02	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-02	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.
OPS-07	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) nécessite au moins trois nœuds de données pour garantir une haute disponibilité et une tolérance aux pannes. Le déploiement d'un domaine de OpenSearch service comportant au moins trois nœuds de données garantit les opérations du cluster en cas de défaillance d'un nœud.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegarde s et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
OPS-07	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-07	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.
OPS-12	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-12	s3-lifecycle-policy-check	Assurez-vous que les politique s de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-13	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-13	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
OPS-14	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
OPS-14	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-14	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
OPS-14	s3-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).
OPS-15	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-15	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
OPS-15	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.
OPS-15	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-15	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
OPS-15	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-15	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
OPS-15	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
OPS-15	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-15	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
OPS-15	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-15	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
OPS-15	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-15	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
OPS-15	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
OPS-22	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.
PSS-05	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifact orielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
PSS-05	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
PSS-05	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
PSS-05	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
PSS-07	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Germany Cloud Computing Compliance Criteria Catalog (C5).

Bonnes pratiques de fonctionnement pour Gramm Leach Bliley Act (GLBA)

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les règles Gramm-Leach-Bliley Act (GLBA) et les règles de configuration gérées par AWS . Chaque règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles GLBA. Un contrôle GLBA peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-sect	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ion (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financièr es soumises à leur juridiction en matière de protectio ns administratives, techniques et physiques		instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-sect ion (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financièr es soumises à leur juridiction en matière de protectio ns administratives, techniques et physiques	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(1)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (1) pour assurer la sécurité et la confidentialité des enregistrements et des informations clients ;	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(2)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (2) pour anticiper et contrer toute menace ou tout risque lié(e) à la sécurité et l'intégrité de ces enregistrements ; et	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(2)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (2) pour anticiper et contrer toute menace ou tout risque lié(e) à la sécurité et l'intégrité de ces enregistrements ; et	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon OpenSearch Service. Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
GLBA-SEC.501(b)(3)	Conformément à la politique énoncée dans la sous-section (a), chaque agence ou autorité décrite dans la section 505(a) doit définir des normes appropriées pour les institutions financières soumises à leur juridiction en matière de protections administratives, techniques et physiques (3) pour contrer tout accès non autorisé à ces enregistrements ou informations, ou toute utilisation non autorisé de ceux-ci, qui pourrait nuire considérablement à un client.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for Gramm Leach Bliley Act (GLBA).

Bonnes pratiques de fonctionnement pour GxP EU Annex 11

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre l'annexe 11 du GxP EU et les règles de configuration AWS gérées. Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles GxP EU Annex 11. Un contrôle GxP EU Annex 11 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1. Gestion des risques	La gestion des risques doit être appliquée tout au long du cycle de vie du système informatisé et tenir compte de la sécurité des patients, de l'intégrité des données et de la qualité des produits. Dans le cadre d'un système de gestion des risques, les décisions concernant l'étendue de la validation et des contrôles de l'intégrité des données	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	devraient être fondées sur une évaluation des risques prouvée et documentée du système informatisé.		sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
1. Gestion des risques	La gestion des risques doit être appliquée tout au long du cycle de vie du système informatisé et tenir compte de la sécurité des patients, de l'intégrité des données et de la qualité des produits. Dans le cadre d'un système de gestion des risques, les décisions concernant l'étendue de la validation et des contrôles de l'intégrité des données devraient être fondées sur une évaluation des risques prouvée et documentée du système informatisé.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.2. Validation - Contrôle des modifications apportées à la documentation	La documentation liée à la validation doit inclure des enregistrements de contrôle des modifications (le cas échéant) et des rapports sur tout écart observé au cours du processus de validation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3. Validation - Inventaire	Une liste actualisée de tous les systèmes concernés et de leurs fonctionnalités GMP (inventaire) doit être fournie. Pour les systèmes critiques , une description actualisée du système détaillant les mesures physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, les prérequis matériels et logiciels, et les mesures de sécurité doit être fournie.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3. Validation - Inventaire	Une liste actualisée de tous les systèmes concernés et de leurs fonctionnalités GMP (inventaire) doit être fournie. Pour les systèmes critiques , une description actualisée du système détaillant les mesures physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, les prérequis matériels et logiciels, et les mesures de sécurité doit être fournie.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3. Validation - Inventaire	Une liste actualisée de tous les systèmes concernés et de leurs fonctionnalités GMP (inventaire) doit être fournie. Pour les systèmes critiques , une description actualisée du système détaillant les mesures physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, les prérequis matériels et logiciels, et les mesures de sécurité doit être fournie.	ec2-security-group-attached-to-eni-periodic	Pour vous aider à gérer votre inventaire d'actifs, cette règle vérifie si des groupes de sécurité sont liés à des instances Amazon Elastic Compute Cloud (Amazon EC2) ou à une interface réseau Elastic. Si vos groupes de sécurité ne sont pas liés à ce type de ressources, il se peut qu'ils ne soient pas utilisés et que vous n'en ayez plus besoin.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3. Validation - Inventaire	Une liste actualisée de tous les systèmes concernés et de leurs fonctionnalités GMP (inventaire) doit être fournie. Pour les systèmes critiques , une description actualisée du système détaillant les mesures physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, les prérequis matériels et logiciels, et les mesures de sécurité doit être fournie.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3. Validation - Inventaire	Une liste actualisée de tous les systèmes concernés et de leurs fonctionnalités GMP (inventaire) doit être fournie. Pour les systèmes critiques , une description actualisée du système détaillant les mesures physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, les prérequis matériels et logiciels, et les mesures de sécurité doit être fournie.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.3. Validation - Inventaire	Une liste actualisée de tous les systèmes concernés et de leurs fonctionnalités GMP (inventaire) doit être fournie. Pour les systèmes critiques , une description actualisée du système détaillant les mesures physiques et logiques, les flux de données et les interfaces avec d'autres systèmes ou processus, les prérequis matériels et logiciels, et les mesures de sécurité doit être fournie.	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.8. Validation - Transfert de données	Si les données sont transférées dans un autre format ou vers un autre système, la validation doit inclure des contrôles montrant que la valeur et/ou la signification des données ne sont pas modifiées au cours du processus de migration.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Données	Les systèmes informatisés échangeant des données avec d'autres systèmes par voie électronique devraient inclure des contrôles intégrés appropriés permettant de saisir et de traiter correctement les données de manière sécurisée, afin de minimiser les risques.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1. Stockage de données - Protection contre les dommages	Les données doivent être protégées physiquement et électroniquement contre tout dommage. L'accessibilité, la lisibilité et l'exactitude des données stockées doivent être vérifiées. L'accès aux données doit être garanti pendant toute la période de conservation.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2. Stockage de données - Sauvegardes	Vous devez réaliser des sauvegardes régulières de toutes les données pertinentes. L'intégrité et la précision des données de sauvegarde, ainsi que la capacité à restaurer les données, doivent être contrôlées lors de la validation et régulièrement surveillées.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Pistes d'audit	Pour évaluer les risques, il faudrait envisager d'intégrer au système un enregistrement de toutes les modifications et suppressions GMP (une « piste d'audit » générée par le système). La raison de chaque modification ou suppression de données GMP doit être documentée. Les pistes d'audit doivent être accessibles et pouvoir être converties en un format standard intelligible. Elles doivent aussi être régulièrement révisées.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Gestion des modifications et des configurations	Toute modification apportée à un système informatisé, y compris aux configurations du système, doit uniquement être effectuée de manière contrôlée conformément à une procédure prédéfinie.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Gestion des modifications et des configurations	Toute modificat ion apportée à un système informatisé, y compris aux configura tions du système, doit uniquement être effectuée de manière contrôlée conformém ent à une procédure prédéfinie.	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Gestion des modifications et des configurations	Toute modificat ion apportée à un système informatisé, y compris aux configura tions du système, doit uniquement être effectuée de manière contrôlée conformém ent à une procédure prédéfinie.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Évaluation régulière	Les systèmes informatisés doivent être régulièrement évalués pour vérifier qu'ils sont toujours en bon état et conformes aux GMP. Ces évaluations devraient inclure, le cas échéant, la gamme de fonctionn alités actuelle, les enregistrements des écarts, les incidents , les problèmes , l'historique des mises à niveau, les performances, la fiabilité, la sécurité et les rapports sur le statut de validation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnel s avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informati que et aux zones de stockage de données.	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnel s avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informati que et aux zones de stockage de données.	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisate ur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnel s avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informati que et aux zones de stockage de données.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearc h Service. Le contrôle d'accès précis fournit des mécanisme s d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authent ification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	rds-instance-iam-authentication-enabled	Assurez-vous qu'une authentification AWS Identity and Access Management (IAM) est activée sur les instances Amazon Relational Database Service (Amazon RDS) afin de contrôler l'accès aux systèmes et aux actifs. Cela permet de chiffrer le trafic réseau à destination et en provenance de la base de données au moyen du protocole SSL. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnel s avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informati que et aux zones de stockage de données.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnels avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informatique et aux zones de stockage de données.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12.1. Sécurité - Personnes autorisées	Des contrôles physiques et/ou logiques doivent être mis en place pour limiter l'accès au système informatisé aux seules personnes autorisées. Pour empêcher toute entrée non autorisée dans le système, il convient d'opter pour l'utilisation de clés, de cartes d'accès, de codes personnel s avec mots de passe ou de données biométriques, et de restreindre l'accès à l'équipement informati que et aux zones de stockage de données.	sagemaker-notebook -no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,3. Sécurité - Piste d'audit des autorisations	Toute création, modification et suppression d'autorisations d'accès doit être enregistrée.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12,4. Sécurité - Piste d'audit	Les systèmes de gestion des données et des documents doivent être capables d'enregistrer l'identité des opérateurs qui saisissent, modifient, valident ou suppriment des données, y compris la date et l'heure.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13. Gestion des incidents	Tous les incidents , et pas seulement les défaillances du système et les erreurs de données, doivent être signalés et évalués. La cause première d'un incident critique doit être identifiée, et des mesures correctiv es et préventives doivent être prises en conséquence.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13. Gestion des incidents	Tous les incidents , et pas seulement les défaillances du système et les erreurs de données, doivent être signalés et évalués. La cause première d'un incident critique doit être identifiée, et des mesures correctiv es et préventives doivent être prises en conséquence.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	backup-recovery-po int-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressource s qui empêche la suppression de points de restaurat ion. L'utilisation d'une politique basée sur les ressource s pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques, des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques, des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiquement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques, des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	lambda-vpc-multi-az-check	Si votre fonction AWS Lambda est configurée pour se connecter à un cloud privé virtuel (VPC) dans votre compte, déployez la fonction AWS Lambda dans au moins deux zones de disponibilité différentes afin de vous assurer que votre fonction est disponible pour traiter les événements en cas d'interruption de service dans une seule zone.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) nécessite au moins trois nœuds de données pour garantir une haute disponibilité et une tolérance aux pannes. Le déploiement d'un domaine de OpenSearch service comportant au moins trois nœuds de données garantit les opérations du cluster en cas de défaillance d'un nœud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternatives doit dépendre du risque, et s'adapter à un système spécifique et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relationa l Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
16. Continuité de l'activité	En ce qui concerne la disponibilité de systèmes informatisés prenant en charge les processus critiques , des dispositions devraient être prises pour garantir la continuité du support de ces processus en cas de panne du système (par exemple un système manuel ou alternatif). Le temps nécessaire pour mettre en œuvre ces solutions alternati ves doit dépendre du risque, et s'adapter à un système spécifiqu e et au processus métier concerné. Ces mesures doivent être correctement documentées et testées.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégri té de ces données doivent être vérifiées . Si des modificat ions pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégri té de ces données doivent être vérifiées . Si des modificat ions pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégri té de ces données doivent être vérifiées . Si des modificat ions pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégri té de ces données doivent être vérifiées . Si des modificat ions pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégri té de ces données doivent être vérifiées . Si des modificat ions pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégri té de ces données doivent être vérifiées . Si des modificat ions pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
17. Archivage	Les données peuvent être archivées. L'accessibilité, la lisibilité et l'intégrité de ces données doivent être vérifiées. Si des modifications pertinentes doivent être apportées au système (par exemple du matériel informatique ou des programmes), la capacité à récupérer les données doit être garantie et testée.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for GxP EU Annex 11.

Bonnes pratiques de fonctionnement pour la sécurité HIPAA

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Health Insurance Portability and Accountability Act (HIPAA) et les règles Managed AWS Config. Chaque règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles HIPAA. Un contrôle HIPAA peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Ce pack de conformité a été validé par AWS Security Assurance Services LLC (AWS SAS), qui est une équipe d'évaluateurs de sécurité qualifiés (QSA) dans le secteur des cartes de paiement, de praticiens certifiés par HITRUST Common Security Framework (CCSFP) et de professionnels de la conformité certifiés pour fournir des conseils et des évaluations pour divers frameworks industriels. AWS Les professionnels de SAS ont conçu ce pack de conformité pour permettre à un client de se conformer à un sous-ensemble de la loi HIPAA.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164,308(a)(1)(ii)(A)	(A) Analyse des risques (obligatoire). Procédez à une évaluation précise et approfondie des potentiels risques et vulnérabilités en matière de confidentialité, d'intégrité et de disponibilité des informations électroniques protégées sur	annual-risk-assessment-performed (Vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	la santé détenues par l'entité couverte.		
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité approprié es pour suffisamm ent et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(1)(ii)(B)	(B) Gestion des risques (obligatoire). Mettez en œuvre des mesures de sécurité appropriées pour suffisamment et correctement réduire les risques et les vulnérabilités conformément à la section 164.306(a).	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensembl e de la main-d'œu vre peut correctem ent accéder aux informations électroni ques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroni ques protégées sur la santé, conformém ent au paragraphe (a) (4) de la présente section, d'y accéder.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées s qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(i)	(3)(i) Norme : sécurité de la main-d'œuvre. Mettez en œuvre des politiques et des procédures pour garantir que l'ensemble de la main-d'œuvre peut correctement accéder aux informations électroniques protégées sur la santé, comme indiqué dans le paragraphe (a)(4) de la présente section, et pour empêcher les membres de la main-d'œuvre qui n'ont pas accès aux informations électroniques protégées sur la santé, conformément au paragraphe (a)(4) de la présente section, d'y accéder.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(A)	(A) Autorisation et/ou surveillance (adressable). Mettez en œuvre des procédures pour autoriser et/ou surveiller les membres de la main-d'œuvre qui travaillent avec des informations électroniques protégées sur la santé ou dans des lieux où elles sont accessibles.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(B)	(B) Procédure d'approbation de la main-d'œuvre (adressable). Mettez en œuvre des procédures pour déterminer si l'accès d'un membre de la main-d'œuvre aux informations électroniques protégées sur la santé est légitime.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(3)(ii)(C)	(C) Procédures de résiliation (adressables). Mettez en œuvre des procédures pour résilier l'accès aux informations électroniques protégées sur la santé lorsque le contrat d'un membre de la main-d'œuvre prend fin ou selon une décision prise conformément au paragraphe (a)(3)(ii)(B) de la présente section.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(i)	(4)(i) Norme : gestion de l'accès aux informations. Mettez en œuvre des politiques et des procédures pour autoriser l'accès aux informations électroniques protégées sur la santé conformément aux exigences applicables de la sous-partie E de la présente section.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(A)	(A) Isolement des fonctions du centre d'échange d'informations sur les soins de santé (obligatoire). Si un centre d'échange d'informations sur les soins de santé fait partie d'une vaste organisation, le centre d'échange doit mettre en œuvre des politiques et des procédures qui protègent ses informations électroniques protégées sur la santé de tout accès non autorisé par d'autres filiales de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(B)	(B) Autorisation d'accès (adressable). Mettez en œuvre des politiques et des procédures pour accorder l'accès aux informations électroniques protégées sur la santé, par exemple, via l'accès à un poste de travail, à une transaction, à un programme, à un processus ou à un autre mécanisme.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(4)(ii)(C)	(C) Création et modification de l'accès (adressable). Mettez en œuvre des politiques et des procédures qui, en se basant sur les politiques d'autorisation d'accès de l'entité, établissent, documentent, examinent et modifient le droit d'accès d'un utilisateur à un poste de travail, à une transaction, à un programme ou à un processus.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(A)	(A) Rappels de sécurité (adressables). Mises à jour de sécurité régulières	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(A)	(A) Rappels de sécurité (adressables). Mises à jour de sécurité régulières	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(A)	(A) Rappels de sécurité (adressables). Mises à jour de sécurité régulières	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(A)	(A) Rappels de sécurité (adressables). Mises à jour de sécurité régulières	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(B)	(B) Protection contre les logiciels malveillants (adressable). Procédures de protection, de détection et de signalement des logiciels malveillants.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(B)	(B) Protection contre les logiciels malveillants (adressable). Procédures de protection, de détection et de signalement des logiciels malveillants.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(B)	(B) Protection contre les logiciels malveillants (adressable). Procédures de protection, de détection et de signalement des logiciels malveillants.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(C)	(C) Surveillance des connexions (adressable). Procédures de surveillance des tentatives de connexion et de signalement des anomalies.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(C)	(C) Surveillance des connexions (adressable). Procédures de surveillance des tentatives de connexion et de signalement des anomalies.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(C)	(C) Surveillance des connexions (adressable). Procédures de surveillance des tentatives de connexion et de signalement des anomalies.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(5)(ii)(D)	(D) Gestion des mots de passe (adressable). Procédures de création, de modification et de sauvegarde des mots de passe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(6)(i)	(6)(i) Norme : procédures relatives aux incidents de sécurité. Mettez en œuvre des politique s et des procédure s pour résoudre les incidents de sécurité.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(6)(ii)	(ii) Spécification de l'implémentation : réponse et rapport (obligatoires). Identifiez et résolvez les incidents de sécurité présumés ou avérés ; atténuez, dans la mesure du possible, les répercussions négatives des incidents de sécurité avérés sur l'entité couverte ; et documentez les incidents de sécurité et leurs conséquences.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(i)	(7)(i) Norme : plan d'urgence. Établissez (et mettez en œuvre si besoin) des politiques et des procédures pour répondre à une situation d'urgence ou tout autre événement (par exemple, un incendie, un acte de vandalisme, une défaillance du système ou une catastrophe naturelle) qui endommagerait les systèmes contenant des informations électroniques protégées sur la santé.	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(A)	(A) Plan de sauvegarde des données (obligatoire). Établissez et mettez en œuvre des procédures permettant de créer et conserver des copies exactes des informations électroniques protégées sur la santé qui pourront être récupérées.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(B)	(B) Plan de reprise après sinistre (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures pour restaurer les données en cas de perte.	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(C)	(C) Plan de fonctionnement d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant de poursuivre les processus opérationnels essentiels pour protéger la sécurité des informations électroniques protégées sur la santé pendant le fonctionnement d'urgence.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(C)	(C) Plan de fonctionnement d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant de poursuivre les processus opérationnels essentiels pour protéger la sécurité des informations électroniques protégées sur la santé pendant le fonctionnement d'urgence.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(C)	(C) Plan de fonctionnement d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant de poursuivre les processus opérationnels essentiels pour protéger la sécurité des informations électroniques protégées sur la santé pendant le fonctionnement d'urgence.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(C)	(C) Plan de fonctionnement d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant de poursuivre les processus opérationnels essentiels pour protéger la sécurité des informations électroniques protégées sur la santé pendant le fonctionnement d'urgence.	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(C)	(C) Plan de fonctionnement d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant de poursuivre les processus opérationnels essentiels pour protéger la sécurité des informations électroniques protégées sur la santé pendant le fonctionnement d'urgence.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(7)(ii)(C)	(C) Plan de fonctionnement d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant de poursuivre les processus opérationnels essentiels pour protéger la sécurité des informations électroniques protégées sur la santé pendant le fonctionnement d'urgence.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(8)	(8) Norme : évaluation. Effectuez régulièrement des évaluations techniques et non techniques, d'abord en vous basant sur les normes mises en œuvre dans le cadre de cette règle, puis sur les changements environnementaux ou opérationnels qui affectent la sécurité des informations électroniques protégées sur la santé, qui mesurent le niveau de conformité des politiques et procédures de sécurité d'une entité par rapport aux exigences de cette sous-partie.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.308(a)(8)	(8) Norme : évaluation. Effectuez régulièrement des évaluations techniques et non techniques, d'abord en vous basant sur les normes mises en œuvre dans le cadre de cette règle, puis sur les changements environnementaux ou opérationnels qui affectent la sécurité des informations électroniques protégées sur la santé, qui mesurent le niveau de conformité des politiques et procédures de sécurité d'une entité par rapport aux exigences de cette sous-partie.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	internet-gateway-a uthorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectée s qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiel lement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	sagemaker-notebook -no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	autoscaling-launch -config-public-ip- disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe 164.308(a)(4).	ecs-containers-rea donly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instanc e de conteneur ne peut être modifié que s'il dispose d'autoris ations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informatiques électroniques qui stockent des informations électroniques protégées sur la santé afin de n'autoriser l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformément au paragraphe 164.308(a)(4).	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(1)	(a)(1) Norme : contrôle d'accès. Mettez en œuvre des politiques et des procédures techniques pour les systèmes informati ques électroniques qui stockent des informations électroni ques protégées sur la santé afin de n'autoris er l'accès qu'aux personnes ou aux logiciels auxquels les droits d'accès ont été accordés conformém ent au paragraphe ¤ 164.308(a)(4).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(i)	(2) Spécifications de l'implémentation : (i) Identification unique de l'utilisa teur (obligatoire). Attribuez des noms et/ou numéros uniques pour identifier et contrôler l'identité des utilisateurs.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(ii)	(ii) Procédure d'accès d'urgence (obligatoire). Établissez (et mettez en œuvre si besoin) des procédures permettant d'accéder aux informations électroniques protégées sur la santé nécessaires en cas d'urgence.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(a)(2)(iv)	(iv) Chiffrement et déchiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer et de déchiffrer les informations électroniques protégées sur la santé.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanismes procéduraux qui enregistrent et analysent l'activité des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanismes procéduraux qui enregistrent et analysent l'activité des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanismes procéduraux qui enregistrent et analysent l'activité des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidente lle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(b)	(b) Norme : contrôles d'audit. Installez du matériel, des logiciels et/ou des mécanisme s procéduraux qui enregistrent et analysent l'activit é des systèmes informatiques contenant ou utilisant des informations électroniques protégées sur la santé.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(1)	(c)(1) Norme : intégrité. Mettez en œuvre des politique s et des procédure s pour protéger les informations électroni ques protégées sur la santé contre toute modification ou suppression inappropr iée.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartim ent Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouill age d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(1)	(c)(1) Norme : intégrité. Mettez en œuvre des politique s et des procédure s pour protéger les informations électroni ques protégées sur la santé contre toute modification ou suppression inappropr iée.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(1)	(c)(1) Norme : intégrité. Mettez en œuvre des politiques et des procédures pour protéger les informations électroniques protégées sur la santé contre toute modification ou suppression inappropriée.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(1)	(c)(1) Norme : intégrité. Mettez en œuvre des politiques et des procédures pour protéger les informations électroniques protégées sur la santé contre toute modification ou suppression inappropriée.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
164.312(c)(1)	(c)(1) Norme : intégrité. Mettez en œuvre des politiques et des procédures pour protéger les informations électroniques protégées sur la santé contre toute modification ou suppression inappropriée.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(2)	(2) Spécifications de l'implémentation : mécanisme d'authentification des informations électroniques protégées sur la santé (adressable). Mettez en œuvre des mécanismes électroniques pour vérifier que les informations électroniques protégées sur la santé n'ont pas été modifiées ou supprimées de manière non autorisée.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(2)	(2) Spécifications de l'implémentation : mécanisme d'authentification des informations électroniques protégées sur la santé (adressable). Mettez en œuvre des mécanismes électroniques pour vérifier que les informations électroniques protégées sur la santé n'ont pas été modifiées ou supprimées de manière non autorisée.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(2)	(2) Spécifications de l'implémentation : mécanisme d'authentification des informations électroniques protégées sur la santé (adressable). Mettez en œuvre des mécanismes électroniques pour vérifier que les informations électroniques protégées sur la santé n'ont pas été modifiées ou supprimées de manière non autorisée.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(2)	(2) Spécifications de l'implémentation : mécanisme d'authentification des informations électroniques protégées sur la santé (adressable). Mettez en œuvre des mécanismes électroniques pour vérifier que les informations électroniques protégées sur la santé n'ont pas été modifiées ou supprimées de manière non autorisée.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(c)(2)	(2) Spécifications de l'implémentation : mécanisme d'authentification des informations électroniques protégées sur la santé (adressable). Mettez en œuvre des mécanismes électroniques pour vérifier que les informations électroniques protégées sur la santé n'ont pas été modifiées ou supprimées de manière non autorisée.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(d)	(d) Norme : authentification d'une personne ou d'une entité. Mettez en œuvre des procédures permettant de vérifier l'identité d'une personne ou une entité souhaitant accéder à des informations électroniques protégées sur la santé.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(d)	(d) Norme : authentification d'une personne ou d'une entité. Mettez en œuvre des procédures permettant de vérifier l'identité d'une personne ou une entité souhaitant accéder à des informations électroniques protégées sur la santé.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(d)	(d) Norme : authentification d'une personne ou d'une entité. Mettez en œuvre des procédures permettant de vérifier l'identité d'une personne ou une entité souhaitant accéder à des informations électroniques protégées sur la santé.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(d)	(d) Norme : authentification d'une personne ou d'une entité. Mettez en œuvre des procédures permettant de vérifier l'identité d'une personne ou une entité souhaitant accéder à des informations électroniques protégées sur la santé.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(d)	(d) Norme : authentification d'une personne ou d'une entité. Mettez en œuvre des procédures permettant de vérifier l'identité d'une personne ou une entité souhaitant accéder à des informations électroniques protégées sur la santé.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(1)	(e)(1) Norme : sécurité des transmissions. Mettez en œuvre des mesures de sécurité techniques pour empêcher l'accès non autorisé aux informations électroniques protégées sur la santé transmises via un réseau de communications électroniques.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(i)	(i) Contrôles d'intégrité (adressables). Mettez en œuvre des mesures de sécurité pour vérifier que les informations électroniques protégées sur la santé transmises électroniquement n'ont pas été modifiées de manière inappropriée et inaperçue avant d'être supprimées.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.312(e)(2)(ii)	(ii) Chiffrement (adressable). Mettez en œuvre un mécanisme permettant de chiffrer les informations électroniques protégées sur la santé dès que nécessaire.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informations électroniques protégées sur la santé divulguées à un promoteur sont transmises conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnable et appropriée les informations électroniques protégées sur la santé créées, reçues, conservées ou transmises par le/au promoteur du plan pour le compte du plan de santé collectif.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	sagemaker-endpoint -configuration-kms- key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(1)	(b)(1) Norme : exigences relatives aux plans de santé collectifs. Excepté si les seules informati ons électroniques protégées sur la santé divulguée s à un promoteur sont transmise s conformément au paragraphe ¤ 164.504(f)(1)(ii) ou (iii), ou comme autorisé en vertu du paragraphe ¤ 164.508, un plan de santé collectif doit comporter des documents qui prévoient que son promoteur protégera de manière raisonnab le et appropriée les informations électroni ques protégées sur la santé créées, reçues, conservées ou transmises par le/ au promoteur du plan pour le compte du plan de santé collectif.	sagemaker-notebook -instance-kms-key- configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-note s, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administr atives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégri té et la disponibi lité des informati ons électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraph e ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité approprié es ; (iii) veiller à ce	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administr atives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégri té et la disponibi lité des informati ons électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraph e ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité approprié es ; (iii) veiller à ce	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informations ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informations ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informations ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administr atives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégri té et la disponibi lité des informati ons électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraph e ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité approprié es ; (iii) veiller à ce	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informations ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ; (ii) veiller à ce que la séparation requise par le paragraphe ¤ 164.504(f)(2) (iii) soit appuyée par des mesures de sécurité appropriées ; (iii) veiller à ce	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	que tout agent, ou sous-traitant, à qui ces informations sont fournies s'engage à mettre en œuvre des mesures de sécurité appropriées pour protéger les informati ons ; et (iv) signaler au plan de santé collectif tout incident de sécurité connu.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classiques utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfinie pour vos écouteurs SSL. La politique de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sécurité par défaut est la suivante : ELB SecurityPolicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisation
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administr atives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégri té et la disponibi lité des informati ons électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administr atives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégri té et la disponibi lité des informati ons électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administr atives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégri té et la disponibi lité des informati ons électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
164.314(b)(2)(i)	(2) Spécifications de l'implémentation (obligatoire). Les documents du plan de santé collectif doivent être modifiés pour intégrer des dispositions obligeant le promoteur à — (i) mettre en œuvre des protections administratives, physiques et techniques qui protègent de manière appropriée la confidentialité, l'intégrité et la disponibilité des informations électroniques protégées sur la santé qu'il crée, reçoit, conserve ou transmet au nom du plan de santé collectif ;	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour la sécurité HIPAA.

Bonnes pratiques de fonctionnement pour IRS 1#075

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou

d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre l'IRS 1075 et les règles de configuration AWS gérées. Chaque règle Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles IRS 1075. Un contrôle IRS 1075 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing d. Chiffrement des données en transit	Les FTI doivent être chiffrées en transit dans l'environnement Cloud. Tous les mécanismes utilisés pour chiffrer les FTI doivent être certifiés FIPS 140 et fonctionner avec les derniers modules conformes à la norme FIPS 140. Cette exigence doit être incluse dans le SLA.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.3.1 Cloud computing d. Chiffrement des données en transit	Les FTI doivent être chiffrées en transit dans l'environnement Cloud. Tous les mécanismes utilisés pour chiffrer les FTI doivent être certifiés	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	FIPS 140 et fonctionner avec les derniers modules conformes à la norme FIPS 140. Cette exigence doit être incluse dans le SLA.		le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.3.1 Cloud computing d. Chiffrement des données en transit	Les FTI doivent être chiffrées en transit dans l'environnement Cloud. Tous les mécanismes utilisés pour chiffrer les FTI doivent être certifiés FIPS 140 et fonctionner avec les derniers modules conformes à la norme FIPS 140. Cette exigence doit être incluse dans le SLA.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing d. Chiffrement des données en transit	Les FTI doivent être chiffrées en transit dans l'environnement Cloud. Tous les mécanismes utilisés pour chiffrer les FTI doivent être certifiés FIPS 140 et fonctionner avec les derniers modules conformes à la norme FIPS 140. Cette exigence doit être incluse dans le SLA.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing d. Chiffrement des données en transit	Les FTI doivent être chiffrées en transit dans l'environnement Cloud. Tous les mécanismes utilisés pour chiffrer les FTI doivent être certifiés FIPS 140 et fonctionner avec les derniers modules conformes à la norme FIPS 140. Cette exigence doit être incluse dans le SLA.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing d. Chiffrement des données en transit	Les FTI doivent être chiffrées en transit dans l'environnement Cloud. Tous les mécanismes utilisés pour chiffrer les FTI doivent être certifiés FIPS 140 et fonctionner avec les derniers modules conformes à la norme FIPS 140. Cette exigence doit être incluse dans le SLA.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.3.1 Cloud computing d. Chiffrement des données en transit	Les FTI doivent être chiffrées en transit dans l'environnement Cloud. Tous les mécanismes utilisés pour chiffrer les FTI doivent être certifiés FIPS 140 et fonctionner avec les derniers modules conformes à la norme FIPS 140. Cette exigence doit être incluse dans le SLA.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing e. Chiffrement des données au repos	Chiffrement des données au repos : lorsqu'elles sont au repos dans le Cloud, les FTI doit être chiffrées à l'aide du mécanisme de chiffrement certifié FIPS 140 le plus récent. Cette exigence doit être incluse dans le SLA.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing k. Authentification multifactorielle	Si leurs solutions Cloud sont accessibles depuis Internet (c'est-à-dire que des individus peuvent y accéder en dehors du réseau sécurisé de l'agence), les agences doivent mettre en place une authentification multifactorielle appropriée.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing k. Authentification multifactorielle	Si leurs solutions Cloud sont accessibles depuis Internet (c'est-à-dire que des individus peuvent y accéder en dehors du réseau sécurisé de l'agence), les agences doivent mettre en place une authentification multifactorielle appropriée.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing k. Authentification multifactorielle	Si leurs solutions Cloud sont accessibles depuis Internet (c'est-à-dire que des individus peuvent y accéder en dehors du réseau sécurisé de l'agence), les agences doivent mettre en place une authentification multifactorielle appropriée.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing k. Authentification multifactorielle	Si leurs solutions Cloud sont accessibles depuis Internet (c'est-à-dire que des individus peuvent y accéder en dehors du réseau sécurisé de l'agence), les agences doivent mettre en place une authentification multifactorielle appropriée.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1 Cloud computing i. Évaluation des risques :	L'agence doit procéder à une évaluation annuelle des contrôles de sécurité et de confidentialité mis en place sur tous les systèmes d'information utilisés pour la réception, le traitement, le stockage, l'accès, la protection et/ou la transmission des FTI.	annual-risk-assessment-performed (vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	netfw-policy-rule-group-associated	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic, et vous définissez la gestion du trafic par défaut.
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.6 Limite du réseau et infrastructure	Les agences doivent adopter des dispositifs de protection des limites dans l'ensemble de leur architecture système, notamment des routeurs, des pare-feu, des commutateurs et des systèmes de détection d'intrusion pour protéger les FTI et les systèmes associés.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (f)	Créez, activez, modifiez, désactivez et supprimez des comptes conformément aux exigences des procédures de gestion des comptes de l'agence ;	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (f)	Créez, activez, modifiez, désactivez et supprimez des comptes conformément aux exigences des procédures de gestion des comptes de l'agence ;	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (f)	Créez, activez, modifiez, désactive z et supprimez des comptes conformém ent aux exigences des procédures de gestion des comptes de l'agence ;	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (f)	Créez, activez, modifiez, désactive z et supprimez des comptes conformém ent aux exigences des procédures de gestion des comptes de l'agence ;	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (f)	Créez, activez, modifiez, désactive z et supprimez des comptes conformém ent aux exigences des procédures de gestion des comptes de l'agence ;	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (g)	Surveillez l'utilisation des comptes	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	secretsmanager-secret-periodic-rotation	Cette règle garantit que AWS la rotation périodique des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis. La valeur par défaut est 90 jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 Gestion des comptes (j)	Vérifiez que les comptes sont conformes aux exigences de gestion des comptes	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
(CE-1) Système automatisé de gestion des comptes	Assurez la gestion des comptes système à l'aide de mécanisme s automatisés.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
(CE-1) Système automatisé de gestion des comptes	Assurez la gestion des comptes système à l'aide de mécanisme s automatisés.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisate urs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourci r la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
(CE-1) Système automatisé de gestion des comptes	Assurez la gestion des comptes système à l'aide de mécanismes automatisés.	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
(CE-3) : désactivation des comptes	Désactivez les comptes sous un délai de 120 jours lorsque les comptes : a. ont expiré ; b. ne sont plus associés à aucun utilisateur ou individu ; c. enfreignent la politique de l'organisation ; ou d. sont inactifs depuis 120 jours (pour les comptes non privilégiés) et 60 jours (pour les comptes privilégiés)	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
(CE-12) Surveillance des comptes en cas d'utilisation anormale	Surveillez les comptes système pour détecter toute utilisation anormale (telle que définie par l'agence) ; et signalez l'utilisa tion anormale des comptes système au personnel ou aux employés définis par l'agence.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisa teur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 Moindre privilège	Appliquez le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
AC-6 Moindre privilège	Appliquez le principe du moindre privilège, en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 : accès à distance	Établissez et documentez les restrictions d'utilisation, les exigences de configuration/connexion et les directives d'implémentation pour chaque type d'accès à distance autorisé ; et autorisez individuellement chaque type d'accès à distance au système avant d'autoriser de telles connexions.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AT-1 : sensibilisation et formation	Formez les utilisateurs système (y compris les gestionnaires, les dirigeants et les sous-traitants) en matière de sécurité et de confidentialité	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
AU-2 : événements d'audit	Identifiez les types d'événements que le système peut journaliser dans le cadre de la fonction d'audit	audit-log-policy-exists (vérification du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisation en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-16 : journalisation des audits entre les organisations	Utilisez les méthodes définies par l'agence pour coordonner les informations d'audit définies par l'agence dans les organisations externes lorsque les informations d'audit sont transmises au-delà des limites de l'organisation.	audit-log-policy-exists (vérification du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisation en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7 : surveillance continue	Élaborez une stratégie de surveillance continue au niveau du système et mettez en œuvre une surveillance continue conformément à la stratégie de surveillance continue définie au niveau de l'organisation : identifiez les mesures définies par l'agence à surveiller ; des évaluations continues des contrôles conformément à la stratégie de surveillance continue ; une surveillance continue du système et des mesures définies par l'organisation conformément à la stratégie de surveillance continue ; la corrélation et l'analyse des informations générées par les évaluations et le suivi des contrôles ; des actions en réponse aux résultats de l'analyse de l'évaluat	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ion des contrôles et des informations de surveillance ; et le signalement de l'état de sécurité et de confidentialité du système au personnel défini par l'agence au moins une fois par an.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	aurora-resources-p rotected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressource s qui empêche la suppression de points de restaurat ion. L'utilisation d'une politique basée sur les ressource s pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documentation du système, y compris la documentation relative à la sécurité ; b. Effectuez des sauvegardes hebdomadaires des informations sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confidentialité ; et d. Assurez la confidentialité, l'intégrité et la disponibilité des informations liées à ces sauvegardes.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9 : sauvegarde du système	a. Effectuez des sauvegardes hebdomadaires des informations sur les utilisateurs présentes dans la documenta tion du système, y compris la documenta tion relative à la sécurité ; b. Effectuez des sauvegard es hebdomada ires des informati ons sur le système présentes dans le système ; c. Effectuez des sauvegardes hebdomadaires de la documentation du système, y compris la documentation relative à la sécurité et à la confident ialité ; et d. Assurez la confidentialité, l'intégri té et la disponibilité des informations liées à ces sauvegardes.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 : identification et authentification (utilisateurs de l'organisation) (CE-1) Authentification multifactorielle pour les comptes privilégiés	Utilisez l'authentification multifactorielle pour accéder aux comptes privilégiés	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 : identification et authentification (utilisateurs de l'organisation) (CE-1) Authentification multifactorielle pour les comptes privilégiés	Utilisez l'authentification multifactorielle pour accéder aux comptes privilégiés	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 : identification et authentification (utilisateurs de l'organisation) (CE-2) Authentification multifactorielle pour les comptes non privilégiés	Utilisez l'authent ification multifact orielle pour accéder aux comptes non privilégiés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 : gestion des authentificateurs : (CE-1) Authentification par mot de passe : pour l'authentification par mot de passe	Appliquez les règles de composition et de complexité suivantes : 1. Utilisez un mot de passe contenant au moins quatorze (14) caractères. 2. Ajoutez une complexité minimale au mot de passe afin qu'il contienne une combinaison de chiffres, de lettres majuscules, de lettres minuscules et de caractères spéciaux. 3. Imposez au moins un (1) changement de caractère lorsque de nouveaux mots de passe sont choisis pour être utilisés. 4. Stockez et transmettez uniquement des mots de passe protégés par chiffrement. 5. Appliquez des restrictions relatives à la durée de vie des mots de passe : i. Un (1) jour minimum et 90 jours maximum.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ii. Les mots de passe des comptes de service expireront au bout de 366 jours (tous inclus).		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PM-5 : inventaire des systèmes	Élaborez un inventaire des systèmes de l'organisation et mettez-le constamment à jour.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PM-5 : inventaire des systèmes	Élaborez un inventaire des systèmes de l'organisation et mettez-le constamment à jour.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PM-5 : inventaire des systèmes	Élaborez un inventaire des systèmes de l'organisation et mettez-le constamment à jour.	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
PM-5 : inventaire des systèmes	Élaborez un inventaire des systèmes de l'organisation et mettez-le constamment à jour.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-5 : surveillance et analyse des vulnérabilités	Surveillez et analysez les vulnérabilités du système et des applications hébergées tous les trente (30) jours, avant d'intégrer un nouveau système d'information au réseau de l'agence, pour valider des mesures correctives, et en cas de détection et de signalement de nouvelles vulnérabilités susceptibles d'affecter le système	vuln-scans-performed(vérification du processus)	Assurez-vous que des analyses de vulnérabilité sont effectuées conformément à vos exigences de conformité. La cadence d'analyse, les outils utilisés et l'utilisation des résultats doivent être définis par votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10 : gestion de la configuration pour les développeurs (e.)	Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10 : gestion de la configuration pour les développeurs (e.)	Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10 : gestion de la configuration pour les développeurs (e.)	Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-10 : gestion de la configuration pour les développeurs (a) (c.)	Gérez la configuration lors de la conceptio n, du développement, de l'implémentation ou de l'exploitation d'un système, d'un composant ou d'un service ; implément ez uniquemen t les modificat ions approuvée s par l'organis ation concernan t le système, le composant ou le service ;	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-4 : informations présentes dans les ressources système partagées	Empêchez le déplacement d'informations non autorisé et imprévu via des ressources système partagées	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibl es au public qui sont séparés des réseaux organisat ionnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquemen t par l'intermé diaire d'interfaces gérées constitué es de dispositifs de protection des limites organisés conformém ent à une architecture de sécurité organisat ionnelle.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibl es au public qui sont séparés des réseaux organisat ionnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquemen t par l'intermé diaire d'interfaces gérées constitué es de dispositifs de protection des limites organisés conformém ent à une architecture de sécurité organisat ionnelle.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibles au public qui sont séparés des réseaux organisationnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibl es au public qui sont séparés des réseaux organisat ionnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquemen t par l'intermé diaire d'interfaces gérées constitué es de dispositifs de protection des limites organisés conformém ent à une architecture de sécurité organisat ionnelle.	sagemaker-notebook -no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites	Surveillez et contrôlez les communications aux limites externes du système et aux limites internes clés du système ; implémentez des sous-réseaux pour les composants du système accessibl es au public qui sont séparés des réseaux organisat ionnels internes ; et Connectez-vous à des réseaux ou à des systèmes d'information externes uniquemen t par l'intermé diaire d'interfaces gérées constitué es de dispositifs de protection des limites organisés conformém ent à une architecture de sécurité organisat ionnelle.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites (CE-9) Limiter le trafic des communications sortantes menaçantes	Détectez et bloquez le trafic des communications sortantes qui constituent une menace pour les systèmes externes ; et Contrôlez l'identité des utilisateurs internes associés aux communications refusées.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites (CE-9) Limiter le trafic des communications sortantes menaçantes	Détectez et bloquez le trafic des communications sortantes qui constituent une menace pour les systèmes externes ; et Contrôlez l'identité des utilisateurs internes associés aux communications refusées.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites (CE-9) Limiter le trafic des communications sortantes menaçantes	Détectez et bloquez le trafic des communications sortantes qui constituent une menace pour les systèmes externes ; et Contrôlez l'identité des utilisateurs internes associés aux communications refusées.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 : protection des limites (telles que définies par IRS)	Les agences doivent mettre en œuvre et gérer la protection des limites (générale ment à l'aide de pare-feu) au niveau des limites d'approba tion. Chaque limite d'approbation doit être surveillée et les communications entre chaque limite doivent être contrôlées.	netfw-policy-rule-group-associated	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic, et vous définissez la gestion du trafic par défaut.
SC-7 : protection des limites (telles que définies par IRS)	Les agences doivent mettre en œuvre et gérer la protection des limites (générale ment à l'aide de pare-feu) au niveau des limites d'approba tion. Chaque limite d'approbation doit être surveillée et les communications entre chaque limite doivent être contrôlées.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 : Intégrité et confidentialité des transmissions (CE-1) Protection par le chiffrement	Mettez en œuvre des mécanismes des chiffrement pour empêcher la divulgation non autorisée d'informations et détecter les modifications apportées aux informations pendant la transmission.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 : Intégrité et confidentialité des transmissions (CE-1) Protection par le chiffrement	Mettez en œuvre des mécanismes des chiffrement pour empêcher la divulgation non autorisée d'informations et détecter les modifications apportées aux informations pendant la transmission.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8 : Intégrité et confidentialité des transmissions (CE-1) Protection par le chiffrement	Mettez en œuvre des mécanismes des chiffrement pour empêcher la divulgation non autorisée d'informations et détecter les modifications apportées aux informations pendant la transmission.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 : Intégrité et confidentialité des transmissions (CE-1) Protection par le chiffrement	Mettez en œuvre des mécanismes des chiffrement pour empêcher la divulgation non autorisée d'informations et détecter les modifications apportées aux informations pendant la transmission.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
SC-8 : Intégrité et confidentialité des transmissions (CE-1) Protection par le chiffrement	Mettez en œuvre des mécanismes des chiffrement pour empêcher la divulgation non autorisée d'informations et détecter les modifications apportées aux informations pendant la transmission.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 : Intégrité et confidentialité des transmissions (CE-1) Protection par le chiffrement	Mettez en œuvre des mécanismes des chiffrement pour empêcher la divulgation non autorisée d'informations et détecter les modifications apportées aux informations pendant la transmission.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8 : Intégrité et confidentialité des transmissions (CE-1) Protection par le chiffrement	Mettez en œuvre des mécanismes des chiffrement pour empêcher la divulgation non autorisée d'informations et détecter les modifications apportées aux informations pendant la transmission.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12 : établissement et gestion des clés de chiffrement	L'agence doit établir et gérer des clés de chiffrement si le chiffrement est utilisé dans le système conformément aux exigences de gestion des clés suivantes : NIST SP 800-57, Recommandation pour la gestion des clés, pour la génération, la distribution, le stockage, l'accès et la suppression de clés.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12 : établissement et gestion des clés de chiffrement	L'agence doit établir et gérer des clés de chiffrement si le chiffrement est utilisé dans le système conformément aux exigences de gestion des clés suivantes : NIST SP 800-57, Recommandation pour la gestion des clés, pour la génération, la distribution, le stockage, l'accès et la suppression de clés.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffreme nt adapté parmi les suivants pour chaque chiffrement spécifiqu e : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configura tion et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signature s numériques est interdite.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffreme nt adapté parmi les suivants pour chaque chiffrement spécifiqu e : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configura tion et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signature s numériques est interdite.	opensearch-node-to -node-encryption-c heck	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffreme nt adapté parmi les suivants pour chaque chiffrement spécifiqu e : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configura tion et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signature s numériques est interdite.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13 : protection par le chiffrement	Implémentez le type de chiffrement adapté parmi les suivants pour chaque chiffrement spécifique : mécanisme de chiffrement certifié FIPS-140 le plus récent, NIST 800-52, directives pour la sélection, la configuration et l'utilisation des implémentations du protocole TLS (Transport Layer Security), chiffrement en transit (chiffrement des charges utiles). L'utilisation du SHA-1 pour les signatures numériques est interdite.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 : authenticité des sessions	Protégez l'authent icité des sessions de communication.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 : protection des informations au repos (CE-1) Protection par le chiffrement	Appliquez des mécanismes de chiffrement pour empêcher la divulgation et la modification non autorisées des FTI au repos pour les systèmes informatiques des utilisateurs finaux (par exemple, ordinateurs de bureau, ordinateurs portables, appareils mobiles, dispositifs de stockage portables et amovibles) dans un espace de stockage non volatil.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 : correction des failles (telles que définies par IRS)	L'agence doit veiller à ce que, lors de la mise sous tension et de la connexion quotidiennes au réseau de l'agence, les postes de travail (tels que définis dans la politique, y compris les connexions à distance utilisant les postes de travail GFE) soient vérifiés pour s'assurer que les correctifs les plus récents approuvés par l'agence ont été appliqués et que tous les correctifs absents ou nouveaux sont appliqués si nécessaire ou vérifiés au moins toutes les 24 heures (sauf les week-ends, les jours fériés, etc.)	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 : correction des failles (telles que définies par IRS)	L'agence doit veiller à ce que, lors de la mise sous tension et de la connexion quotidiennes au réseau de l'agence, les postes de travail (tels que définis dans la politique, y compris les connexions à distance utilisant les postes de travail GFE) soient vérifiés pour s'assurer que les correctifs les plus récents approuvés par l'agence ont été appliqués et que tous les correctifs absents ou nouveaux sont appliqués si nécessaire ou vérifiés au moins toutes les 24 heures (sauf les week-ends, les jours fériés, etc.)	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 : correction des failles (telles que définies par IRS)	L'agence doit veiller à ce que, lors de la mise sous tension et de la connexion quotidiennes au réseau de l'agence, les postes de travail (tels que définis dans la politique, y compris les connexions à distance utilisant les postes de travail GFE) soient vérifiés pour s'assurer que les correctifs les plus récents approuvés par l'agence ont été appliqués et que tous les correctifs absents ou nouveaux sont appliqués si nécessaire ou vérifiés au moins toutes les 24 heures (sauf les week-ends, les jours fériés, etc.)	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 : correction des failles (telles que définies par IRS)	L'agence doit veiller à ce que, lors de la mise sous tension et de la connexion quotidiennes au réseau de l'agence, les postes de travail (tels que définis dans la politique, y compris les connexions à distance utilisant les postes de travail GFE) soient vérifiés pour s'assurer que les correctifs les plus récents approuvés par l'agence ont été appliqués et que tous les correctifs absents ou nouveaux sont appliqués si nécessaire ou vérifiés au moins toutes les 24 heures (sauf les week-ends, les jours fériés, etc.)	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 : correction des failles (telles que définies par IRS)	L'agence doit veiller à ce que, lors de la mise sous tension et de la connexion quotidiennes au réseau de l'agence, les postes de travail (tels que définis dans la politique, y compris les connexions à distance utilisant les postes de travail GFE) soient vérifiés pour s'assurer que les correctifs les plus récents approuvés par l'agence ont été appliqués et que tous les correctifs absents ou nouveaux sont appliqués si nécessaire ou vérifiés au moins toutes les 24 heures (sauf les week-ends, les jours fériés, etc.)	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 : correction des failles (telles que définies par IRS)	L'agence doit veiller à ce que, lors de la mise sous tension et de la connexion quotidiennes au réseau de l'agence, les postes de travail (tels que définis dans la politique, y compris les connexions à distance utilisant les postes de travail GFE) soient vérifiés pour s'assurer que les correctifs les plus récents approuvés par l'agence ont été appliqués et que tous les correctifs absents ou nouveaux sont appliqués si nécessaire ou vérifiés au moins toutes les 24 heures (sauf les week-ends, les jours fériés, etc.)	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système	L'organisation : a. Surveille le système d'informa tion pour détecter : 1. Les attaques et les indicateurs d'attaques potentiel les conformément à [Attribution : objectifs de surveillance définis par l'organisation] ; et 2. Les connexion s locales, du réseau et à distance non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c.Déploie des dispositi fs de surveillance : 1. Stratégiquement au sein du système d'information pour recueillir des informati ons essentielles telles que définies par l'organisation ; et 2. À des endroits ponctuels du système	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	pour suivre des types spécifiques de transactions présentant un intérêt pour l'organisation ; d.Protège les informations obtenues à l'aide d'outils de surveillance des intrusions contre tout accès, et toute modification ou suppression non autorisés ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système	L'organisation : a. Surveille le système d'informa tion pour détecter : 1. Les attaques et les indicateurs d'attaques potentiel les conformément à [Attribution : objectifs de surveillance définis par l'organisation] ; et 2. Les connexion s locales, du réseau et à distance non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c.Déploie des dispositi fs de surveillance : 1. Stratégiquement au sein du système d'information pour recueillir des informati ons essentielles telles que définies par l'organisation ; et 2. À des endroits ponctuels du système	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	pour suivre des types spécifiques de transactions présentant un intérêt pour l'organisation ; d.Protège les informations obtenues à l'aide d'outils de surveillance des intrusions contre tout accès, et toute modification ou suppression non autorisés ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système	L'organisation : a. Surveille le système d'information pour détecter : 1. Les attaques et les indicateurs d'attaques potentiel les conformément à [Attribution : objectifs de surveillance définis par l'organisation] ; et 2. Les connexion s locales, du réseau et à distance non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c.Déploie des dispositi fs de surveillance : 1. Stratégiquement au sein du système d'information pour recueillir des informati ons essentielles telles que définies par l'organisation ; et 2. À des endroits ponctuels du système	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	pour suivre des types spécifiques de transactions présentant un intérêt pour l'organisation ; d.Protège les informations obtenues à l'aide d'outils de surveillance des intrusions contre tout accès, et toute modification ou suppression non autorisés ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système	L'organisation : a. Surveille le système d'informa tion pour détecter : 1. Les attaques et les indicateurs d'attaques potentiel les conformément à [Attribution : objectifs de surveillance définis par l'organisation] ; et 2. Les connexion s locales, du réseau et à distance non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c.Déploie des dispositi fs de surveillance : 1. Stratégiquement au sein du système d'information pour recueillir des informati ons essentielles telles que définies par l'organisation ; et 2. À des endroits ponctuels du système	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	pour suivre des types spécifiques de transactions présentant un intérêt pour l'organisation ; d.Protège les informations obtenues à l'aide d'outils de surveillance des intrusions contre tout accès, et toute modification ou suppression non autorisés ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système	L'organisation : a. Surveille le système d'informa tion pour détecter : 1. Les attaques et les indicateurs d'attaques potentiel les conformément à [Attribution : objectifs de surveillance définis par l'organisation] ; et 2. Les connexion s locales, du réseau et à distance non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c.Déploie des dispositi fs de surveillance : 1. Stratégiquement au sein du système d'information pour recueillir des informati ons essentielles telles que définies par l'organisation ; et 2. À des endroits ponctuels du système	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	pour suivre des types spécifiques de transactions présentant un intérêt pour l'organisation ; d.Protège les informations obtenues à l'aide d'outils de surveillance des intrusions contre tout accès, et toute modification ou suppression non autorisés ;		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 : surveillance du système (telle que définie par IRS)	Tous les points/portails d'accès liés à Internet doivent collecter et conserver, pendant au moins un an, les informations d'en-tête des trafics entrant et sortant, excepté pour les connexions Internet « anonymes » approuvées, par exemple par le RSSI de l'agence.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 : intégrité des logiciels, des microprogrammes et des informations	Utilisez des outils de vérification de l'intégrité pour détecter les modifications non autorisées apportées aux logiciels, microprogrammes et informations suivants : noyaux du système, pilotes, microprogrammes (par exemple, BIOS, UEFI), logiciels (par exemple, système d'exploitation, applications, intergiciels) et attributs de sécurité.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 : intégrité des logiciels, des microprogrammes et des informations	Utilisez des outils de vérification de l'intégrité pour détecter les modifications non autorisées apportées aux logiciels, microprogrammes et informations suivants : noyaux du système, pilotes, microprogrammes (par exemple, BIOS, UEFI), logiciels (par exemple, système d'exploitation, applications, intergiciels) et attributs de sécurité.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 : intégrité des logiciels, des microprogrammes et des informations	Utilisez des outils de vérification de l'intégrité pour détecter les modifications non autorisées apportées aux logiciels, microprogrammes et informations suivants : noyaux du système, pilotes, microprogrammes (par exemple, BIOS, UEFI), logiciels (par exemple, système d'exploitation, applications, intergiciels) et attributs de sécurité.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	dynamodb-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'informa tion et les informati ons produites par le système conformément aux lois fédérales, aux décrets, aux directive s, aux règlement s, aux politiques, aux normes, aux consignes et aux exigences opération nelles applicables.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	ebs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'informa tion et les informati ons produites par le système conformément aux lois fédérales, aux décrets, aux directive s, aux règlement s, aux politiques, aux normes, aux consignes et aux exigences opération nelles applicables.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	efs-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'informa tion et les informati ons produites par le système conformément aux lois fédérales, aux décrets, aux directive s, aux règlement s, aux politiques, aux normes, aux consignes et aux exigences opération nelles applicables.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	rds-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'informa tion et les informati ons produites par le système conformément aux lois fédérales, aux décrets, aux directive s, aux règlement s, aux politiques, aux normes, aux consignes et aux exigences opération nelles applicables.	s3-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'informa tion et les informati ons produites par le système conformément aux lois fédérales, aux décrets, aux directive s, aux règlement s, aux politiques, aux normes, aux consignes et aux exigences opération nelles applicables.	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux règlements, aux politiques, aux normes, aux consignes et aux exigences opérationnelles applicables.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12 : gestion et conservation des informations	Gérez et conservez les informations présentes dans le système d'informa tion et les informati ons produites par le système conformément aux lois fédérales, aux décrets, aux directive s, aux règlement s, aux politiques, aux normes, aux consignes et aux exigences opération nelles applicables.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartim ent Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouill age d'objet au repos pour protéger ces données.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for IRS 1075.

Bonnes pratiques de fonctionnement pour K-ISMS

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le système de gestion de la sécurité de l'information (ISMS) coréen et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une ressource AWS spécifique et concerne un ou plusieurs contrôles Korea – ISMS.

Un contrôle Korea – ISMS peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
1.2.1	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
1.2.1	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
2.1.3	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
2.1.3	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
2.3.3	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
2.3.3	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	access-keys-rotated	Les informations d'identif ication sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organis ation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
2.5.1	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
2.5.1	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifact orielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
2.5.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.1	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
2.5.1	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.3	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
2.5.3	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.3	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
2.5.4	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
2.5.5	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'associa tion d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
2.5.5	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
2.5.5	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
2.6	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
2.6	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifact orielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
2.6	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communica tion sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
2.6	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
2.6	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
2.6	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
2.6	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
2.6	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
2.6	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
2.6	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
2.6.6	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
2.6.6	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
2.6.6	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
2.6.6	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
2.6.6	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
2.6.6	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.6.6	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.6.6	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
2.6.6	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
2.6.6	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
2.6.6	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
2.6.6	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
2.6.7	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
2.7	acm-certificate-expiration-check	Assurez-vous que l'intégri té du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleure s pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.7	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
2.7	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
2.7	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.7	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
2.7	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
2.7	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
2.7	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
2.7	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
2.7	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
2.7	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
2.7	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
2.7	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
2.7	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
2.7	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.7	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
2.7	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.7	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
2.7	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
2.7	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.7	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
2.7	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.7	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
2.7	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearc h Service.
2.7	opensearch-node-to-node-enc ryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.7.1	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
2.7.1	elb-predefined-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs SSL Elastic Load Balancer classique s utilisent une politique de sécurité prédéfinie. Elastic Load Balancing fournit des configurations de négociati on SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociati on SSL assurent la compatibi lité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée. Cette règle exige que vous définissiez une politique de sécurité prédéfini e pour vos écouteurs SSL. La politique de sécurité par défaut est la suivante : ELB SecurityP olicy -TLS-1-2-2017-0. La valeur réelle doit refléter les politiques de votre organisat ion
2.7.2	cmk-backing-key-rotation-en abled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	AWS Règle de configuration	Conseils
2.7.2	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
2.8.5	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	AWS Règle de configuration	Conseils
2.8.5	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
2.8.6	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	AWS Règle de configuration	Conseils
2.8.6	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
2.9.1	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.1	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activat ion de plusieurs paramètre s. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrai l l'activation dans plusieurs régions.
2.9.1	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégri té des CloudTrail journaux. La validation du fichier journal permet de détermine r si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison . Cette fonctionnalité est créée grâce à des algorithm es standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.1	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.2	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.2	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.2	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU Threshold Percentage (Config Default : 80). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.2	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.
2.9.2	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.2	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
2.9.3	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
2.9.3	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
2.9.3	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
2.9.3	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	s3-bucket-default-lock-enabled	Assurez-vous que le verrouill age est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartim ents S3, appliquez le verrouill age d'objet au repos pour protéger ces données.
2.9.3	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.3	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.
2.9.4	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.4	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
2.9.4	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
2.9.4	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.4	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
2.9.4	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.4	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
2.9.4	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
2.9.4	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.
2.9.4	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
2.10.3	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.
2.10.3	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
2.10.3	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.10.3	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
2.10.3	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2,1,5	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
2,1,5	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
2,1,5	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2,1,5	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
2,1,5	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
2,1,5	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2,1,5	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
2,1,5	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.10.8	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
2.10.8	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
2.11.2	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
2.11.3	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.
2.11.3	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.

ID du contrôle	AWS Règle de configuration	Conseils
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
2.11.3	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	AWS Règle de configuration	Conseils
2.11.3	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	AWS Règle de configuration	Conseils
2.11.3	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
2,12	db-instance-backup-enabled	La fonctionnalité de sauvegard e d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
2,12	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
2,12	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
2,12	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
2,12	s3-bucket-default-lock-enabled	Assurez-vous que le verrouill age est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartim ents S3, appliquez le verrouill age d'objet au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
2,12	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponi ble. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indispo nibilité de votre passerelle client, vous pouvez configure r une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2,12	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for K-ISMS.

Bonnes pratiques de fonctionnement pour l'équilibrage de charge

Ce pack de conformité contient des AWS Config règles basées sur l'équilibrage de charge intégré. AWS Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour l'équilibrage de charge.

Bonnes pratiques de fonctionnement pour la journalisation

Ce pack de conformité contient des AWS Config règles basées sur la connexion interne AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for Logging.

Bonnes pratiques de fonctionnement pour les services de gestion et de gouvernance

Ce pack de conformité contient des AWS Config règles basées sur les services de gestion et de gouvernance. Pour plus d'informations, consultez la section Gestion et gouvernance sur AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les services de gestion et de gouvernance.

Bonnes pratiques de fonctionnement pour MAS Notice 655

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou

d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de correspondance entre la notice 655 de l'Autorité monétaire de Singapour (MAS) sur l'hygiène informatique et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles MAS Notice 655 — Cyber Hygiene. Un contrôle MAS Notice 655 – Cyber Hygiene peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
4.1	access-keys-rotated	Les informations d'identif ication sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organis ation. La modification régulière des clés d'accès est une

ID du contrôle	AWS Règle de configuration	Conseils
		bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
4.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
4.1	root-account-mfa-enabled	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilège s dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identif ication de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
4.1	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'associa tion d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisate ur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommand e d'utiliser des politiques gérées plutôt que des politique s intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedAc tionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decry pt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
4.1	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
4.1	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
4.1	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
4.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
4.1	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
4.1	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
4.2	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
4.2	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
4.2	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
4.2	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4.2	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
4.2	elastic-beanstalk-managed-u pdates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
4.2	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.
4.2	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	AWS Règle de configuration	Conseils
4.3	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
4.3	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
4.3	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
4.3	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.
4,4	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
4,4	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
4,4	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
4,4	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
4,4	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.
4,4	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communica tion sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
4,4	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
4,4	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.
4,4	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.
4,4	netfw-policy-default-action-fragment-packets	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic. L'utilisation par défaut d'une action Pass peut entraîner un trafic non prévu.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	netfw-policy-default-action-full-packets	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic. L'utilisation par défaut d'une action Pass peut entraîner un trafic non prévu.
4,4	netfw-policy-rule-group-associated	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic, et vous définissez la gestion du trafic par défaut.
4,4	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
4,4	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
4,4	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
4,4	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
4,4	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
4,4	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
4,4	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
4,4	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	AWS Règle de configuration	Conseils
4,4	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
4,4	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	AWS Règle de configuration	Conseils
4,4	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
4,5	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
4,5	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
4,5	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
4,5	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
4.6	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
4.6	root-account-mfa-enabled	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilège s dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identif ication de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
4.6	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
4.6	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
4.6	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
4.6	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for MAS Notice 655.

Bonnes pratiques de fonctionnement pour MAS TRMG

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de correspondance entre les directives de gestion des risques technologiques (TRMG) de janvier 2021 de l'Autorité monétaire de Singapour (MAS) et les règles de AWS configuration gérées. Chaque règle de AWS Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles MAS TRMG. Un contrôle MAS TRMG de janvier 2021 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
3.3.1	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
5.4.3	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et

ID du contrôle	AWS Règle de configuration	Conseils
		AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
5.4.3	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
6.1.1	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	AWS Règle de configuration	Conseils
6.1.2	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
6.1.4	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
6.1.4	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
6.1.4	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
6.2.1	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
6.3.1	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.5	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
6.4.5	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
6.4.5	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.5	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.
6.4.5	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
6.4.5	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.5	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
6.4.5	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
6.4.5	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.5	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
6.4.5	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
6.4.5	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
6.4.6	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
6.4.6	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.6	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
6.4.7	api-gw-execution-logging-en abled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
6.4.7	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatc h pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
6.4.7	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
6.4.7	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
6.4.7	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
6.4.8	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augment er sa capacité de lecture/ d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.8	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
6.4.8	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.8	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.
6.4.8	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.8	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.8	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
6.4.8	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
7.2.1	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
7.2.1	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
7.4.1	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
7.4.1	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
7.4.1	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
7.4.1	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
7.4.1	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
7.4.1	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
7.5.5	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
7.5.5	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
7.5.5	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.
7.5.5	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
7.5.5	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
7.5.5	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
7.5.5	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
7.5.5	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
7.5.5	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
7.5.5	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
7,5.7	api-gw-execution-logging-en abled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
7,5.7	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatc h pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
7,5.7	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
7,5.7	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
7,5.7	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
7,5.7	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
7,5.7	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
7,5.7	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
7,5.7	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
7,5.7	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
7,5.7	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
7,5.7	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
8.1.1	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.1	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.
8.1.1	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.1	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.
8.1.1	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.1	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.1	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.1	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponi ble. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indispo nibilité de votre passerelle client, vous pouvez configure r une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.2	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.2	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.2	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
8.1.2	opensearch-data-node-fault-tolerance	Amazon OpenSearch Service (OpenSearch Service) nécessite au moins trois nœuds de données pour garantir une haute disponibilité et une tolérance aux pannes. Le déploiement d'un domaine de OpenSearch service comportant au moins trois nœuds de données garantit les opérations du cluster en cas de défaillance d'un nœud.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.2	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.3	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.3	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modificat ions de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'applica tion. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifié s et d'identifier les causes possibles à étudier.
8.1.3	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatc h pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
8.1.3	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
8.4.1	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.1	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
8.4.1	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.1	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
8.4.1	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémen taire dédiée aux opération s d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opération s d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.1	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.1	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.1	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.
8.4.1	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.1	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
8.4.1	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.2	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
8.4.2	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.2	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.
8.4.2	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.2	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémen taire dédiée aux opération s d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opération s d'E/S d'Amazon EBS et le trafic restant de votre instance.
8.4.2	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.2	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.2	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.2	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantan és de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventuali té.
8.4.2	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
8.4.2	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.
8.4.4	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
8.5.4	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
8.5.4	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
9.1.1	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'associa tion d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
9.1.1	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
9.1.1	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
9.1.1	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
9.1.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
9.1.1	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctem ent transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
9.1.1	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.1	secretsmanager-secret-periodic-rotation	Cette règle garantit que AWS la rotation périodique des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis. La valeur par défaut est 90 jours.
9.1.1	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
9.1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.2	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.2	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.2	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
9.1.3	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
9.1.3	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
9.1.3	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
9.1.3	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
9.1.3	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
9.1.3	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.3	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.4	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
9.1.5	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifact orielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.5	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.5	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
9.1.5	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
9.1.6	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.7	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.7	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
9.1.7	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.7	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.1.7	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.1	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
9.2.1	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
9.2.1	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.1	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
9.2.1	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.1	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.1	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
9.2.1	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.1	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.1	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
9.2.2	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.2	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
9.2.2	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
9.2.2	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.2	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.2	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
9.2.2	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.2	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.2.2	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
9.3.1	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
9.3.1	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
9.3.1	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
9.3.1	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
9.3.1	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
9.3.1	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
9.3.1	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
9.3.1	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
10.1.1	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
10.1.1	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
10.1.1	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
10.1.1	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
10.1.1	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
10.1.1	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
10.1.1	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
10.1.1	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearc h Service.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
10.1.1	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
10.1.1	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
10.1.1	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
10.1.1	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
10.1.1	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
10.1.1	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
10.1.1	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
10.1.1	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
10.1.1	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
10.1.1	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
10.1.1	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
10.2.1	acm-certificate-expiration-check	Assurez-vous que l'intégri té du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleure s pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politique s de votre organisation.
10.2.1	cmk-backing-key-rotation-en abled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	AWS Règle de configuration	Conseils
10.2.1	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
10.2.2	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	AWS Règle de configuration	Conseils
10.2.3	access-keys-rotated	Les informations d'identif ication sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organis ation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.
10.2.3	cmk-backing-key-rotation-en abled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	AWS Règle de configuration	Conseils
10.2.3	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
11.1.1 (a)	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (a)	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
11.1.1 (a)	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
11.1.1 (a)	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (a)	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
11.1.1 (a)	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (a)	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
11.1.1 (a)	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (a)	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
11.1.1 (b)	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
11.1.1 (b)	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
11.1.1 (b)	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
11.1.1 (b)	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
11.1.1 (b)	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.1.1 (b)	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.1.1 (b)	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
11.1.1 (b)	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
11.1.1 (b)	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
11.1.1 (b)	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
11.1.1 (b)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerell e Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
11.1.1 (b)	rds-instance-public-access-check	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
11.1.1 (b)	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
11.1.1 (b)	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
11.1.1 (b)	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
11.1.1 (b)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
11.1.1 (b)	s3-bucket-public-read-prohi bited	Gérez l'accès aux ressource s dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartim ents Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classific ation des données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
11.1.1 (b)	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
11.1.1 (b)	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
11.1.1 (b)	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
11.1.1 (b)	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
11.1.1 (b)	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involonta ire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
11.1.3	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
11.1.3	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
11.1.3	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.1.3	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
11.1.3	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
11.1.3	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
11.1.3	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
11.1.3	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi que d'autres informations administratives sur chaque principal.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
11.1.3	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
11.1.3	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.
11.1.3	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
11.1.3	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
11.1.3	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
11.1.3	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
11.1.3	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
11.1.3	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
11.1.3	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
11.2.1	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
11.2.2	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.2.2	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.2.2	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
11.2.2	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
11.2.2	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
11.2.2	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
11.2.2	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
11.2.2	s3-bucket-public-read-prohi bited	Gérez l'accès aux ressource s dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartim ents Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classific ation des données.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
11.2.2	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
11.2.2	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.2	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
11.2.4	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.2.4	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.2.4	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
11.2.4	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
11.2.4	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
11.2.4	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
11.2.4	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
11.2.4	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
11.2.4	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
11.2.4	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
11.2.4	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.
11.3.1	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	AWS Règle de configuration	Conseils
11,3.5	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
11,3.5	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
11,3.5	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
11,3.5	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
11.4.2	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
11.4.2	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
11.4.2	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
11.4.2	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
11.5.2	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
12.1.1	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	AWS Règle de configuration	Conseils
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
12.1.1	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
12.2.2	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
12.2.2	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
12.2.2	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
12.2.2	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
12.2.2	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
12.2.2	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.2	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
12.2.4	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
12,2.5	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	AWS Règle de configuration	Conseils
12,2.5	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
12,2.5	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
12,2.5	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
12.3.2	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
14.1.2	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
14.1.2	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
14.1.2	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
14.1.2	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
14.1.2	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
14.1.2	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
14.1.2	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
14.1.2	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
14.1.2	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
14.1.3	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
14.1.3	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
14.1.3	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
14.2.2	acm-certificate-expiration-check	Assurez-vous que l'intégri té du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleure s pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
14.2.2	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles , activez le chiffrement en transit pour protéger ces données.
14.2.2	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
14.2.2	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
14.2.2	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
14.2.2	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
14.2.2	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
14.2.2	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
14.2.2	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearc h Service.
14.2.2	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
14.2.2	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
14.2.2	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
14.2.6	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
14.2.6	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
14.2.6	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
14.2.6	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
14.2.6	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearc h Service.
14.2.6	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
14.2.6	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
14.2.6	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for MAS TRMG.

Bonnes pratiques de fonctionnement pour la surveillance

Ce pack de conformité contient des AWS Config règles basées sur la surveillance interne AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for Monitoring.

Bonnes pratiques de fonctionnement pour NBC TRMG

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de correspondance entre le cadre des directives de gestion des risques technologiques (TRM) de la Banque nationale du Cambodge (NBC) et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne une ou plusieurs directives NBC TRM. Un cadre NBC TRM Guideline peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages avec des contrôles au sein du cadre National Bank of Cambodia's (NBC) Technology Risk Management (TRM) Guidelines, accessible via le lien suivant : National Bank of Cambodia: Technology Risk Mangement Guidelines.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus		teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	cw-loggroup-retent ion-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisant e pour faciliter le dépannage et les enquêtes judiciair es. Le manque de données disponibl es dans les journaux d'événements passés complique la reconstit ution et l'identification des événement s potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identifiants d'utilisateur, et la matrice de contrôle d'accès - La réalisation d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparation efficace des tâches - La modification des noms d'utilisateur et/ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifiants d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	iam-user-unused-cr edentials-check	AWS Identity and Access Managemen t (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCreden tialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	account-part-of-or ganizations	La gestion centralis ée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernan ce centralisée des comptes peut entraîner des configura tions de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	iam-user-group-mem bership-check	AWS Identity and Access Managemen t (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisate urs plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identifiants d'utilisateur, et la matrice de contrôle d'accès - La réalisation d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparation efficace des tâches - La modification des noms d'utilisateur et/ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifiants d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(d)	d) Parmi les contrôles importants à prendre en compte figurent : - Un processus systématique visant à appliquer et autoriser la création d'identif iants d'utilisateur, et la matrice de contrôle d'accès - La réalisati on d'une évaluation des risques et l'octroi de droits d'accès selon les résultats obtenus. - La mise en œuvre d'un contrôle d'accès basé sur les rôles conçu pour garantir une séparatio n efficace des tâches - La modification des noms d'utilisateur et/ ou mots de passe par défaut des systèmes, et l'interdiction du partage des identifia nts d'utilisateur et des mots de passe des comptes génériques - La modification des droits d'accès en cas de changement de rôle ou de responsab	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ilité, et la suppressi on des droits d'accès en cas de cessation d'emploi/de contrat - Des processus permettant de notifier en temps opportun l'équipe chargée de la sécurité des informati ons en cas d'ajouts, de suppressions et de changements de rôle d'un utilisate ur - Le rapproche ment périodiqu e des identifiants d'utilisateur dans un système pour identifier les utilisate urs qui ont besoin de ce droit d'accès, et la suppression des identifiants qui n'ont pas besoin de cet accès (si nécessaire) - L'audit, la journalis ation et la surveillance de l'accès aux actifs informatiques par tous les utilisateurs - La désactivation potentiel le des identifiants des utilisateurs d'applica		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	tions critiques qui sont en congé prolongé		
3.1.1(f)	f) À des fins de responsabilisation , assurez-vous que les utilisateurs et les actifs informati ques sont identifiés de façon unique, et que leurs actions sont vérifiables.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(f)	f) À des fins de responsabilisation , assurez-vous que les utilisateurs et les actifs informati ques sont identifiés de façon unique, et que leurs actions sont vérifiables.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.1.1(f)	f) À des fins de responsabilisation , assurez-vous que les utilisateurs et les actifs informati ques sont identifiés de façon unique, et que leurs actions sont vérifiables.	opensearch-audit-l ogging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearc h Service. La journalis ation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification , les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.
3.1.1(f)	f) À des fins de responsabilisation , assurez-vous que les utilisateurs et les actifs informati ques sont identifiés de façon unique, et que leurs actions sont vérifiables.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisate urs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(f)	f) À des fins de responsabilisation , assurez-vous que les utilisateurs et les actifs informati ques sont identifiés de façon unique, et que leurs actions sont vérifiables.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(f)	f) À des fins de responsabilisation , assurez-vous que les utilisateurs et les actifs informati ques sont identifiés de façon unique, et que leurs actions sont vérifiables.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(f)	f) À des fins de responsabilisation , assurez-vous que les utilisateurs et les actifs informati ques sont identifiés de façon unique, et que leurs actions sont vérifiables.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administr ateurs système, les responsables de la sécurité, les programmeurs et la main-d'œu vre effectuant des opérations critiques sont automatiq uement en mesure de causer de graves dommages aux systèmes financier s qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroiteme nt supervisée et toutes les activités liées aux systèmes doivent être enregistr ées, car elle dispose des connaissa nces d'initiés et des ressources nécessair es pour contourne r les contrôles et les procédures de	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administr ateurs système, les responsables de la sécurité, les programmeurs et la main-d'œu vre effectuant des opérations critiques sont automatiq uement en mesure de causer de graves dommages aux systèmes financier s qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroiteme nt supervisée et toutes les activités liées aux systèmes doivent être enregistr ées, car elle dispose des connaissa nces d'initiés et des ressources nécessair es pour contourne r les contrôles et les procédures de	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administr ateurs système, les responsables de la sécurité, les programmeurs et la main-d'œu vre effectuant des opérations critiques sont automatiq uement en mesure de causer de graves dommages aux systèmes financier s qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroiteme nt supervisée et toutes les activités liées aux systèmes doivent être enregistr ées, car elle dispose des connaissa nces d'initiés et des ressources nécessair es pour contourne r les contrôles et les procédures de	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administrateurs système, les responsables de la sécurité, les programmeurs et la main-d'œuvre effectuant des opérations critiques sont automatiquement en mesure de causer de graves dommages aux systèmes financiers qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroitement supervisée et toutes les activités liées aux systèmes doivent être enregistrées, car elle dispose des connaissances d'initiés et des ressources nécessaires pour contourner les contrôles et les procédures de	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administr ateurs système, les responsables de la sécurité, les programmeurs et la main-d'œu vre effectuant des opérations critiques sont automatiq uement en mesure de causer de graves dommages aux systèmes financier s qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroiteme nt supervisée et toutes les activités liées aux systèmes doivent être enregistr ées, car elle dispose des connaissa nces d'initiés et des ressources nécessair es pour contourne r les contrôles et les procédures de	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1(h)	h) Les administr ateurs système, les responsables de la sécurité, les programmeurs et la main-d'œu vre effectuant des opérations critiques sont automatiq uement en mesure de causer de graves dommages aux systèmes financier s qu'ils gèrent ou exploitent, en raison de leurs fonctions et de leur accès privilégié. La main-d'œuvre disposant de droits d'accès élevés au système doit être étroiteme nt supervisée et toutes les activités liées aux systèmes doivent être enregistr ées, car elle dispose des connaissa nces d'initiés et des ressources nécessair es pour contourne r les contrôles et les procédures de	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurité. Certaines pratiques de contrôle et de sécurité énumérées ci-dessous doivent être prises en compte : - La mise en œuvre de l'authentification à deux facteurs pour les utilisateurs privilégiés - La mise en place de contrôles stricts concernant l'accès à distance des utilisateurs privilégiés - La limitation du nombre d'utilisateurs privilégiés - L'octroi d'accès privilégiés ponctuels au besoin - La création d'un journal d'audit regroupant les activités du système réalisées par les utilisateurs privilégiés - Vérifier que les utilisateurs privilégiés n'ont pas accès aux journaux des systèmes dans lesquels leurs activités sont enregistrées - La réalisation d'audits		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ou de révision des journaux à intervall es réguliers - L'interdi ction du partage des identifiants privilégi és et des codes d'accès associés - L'interdiction pour les fournisse urs et les sous-traitants d'obtenir un accès privilégi é aux systèmes sans supervisi on ni surveillance étroites - La protectio n des données de sauvegarde contre tout accès non autorisé		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(a)	a) Le service BFI doit installer des dispositifs de sécurité réseau, tels que des pare-feu, des logiciels antivirus et contre les programmes malveillants, ainsi que des systèmes de détection et de prévention des intrusions, au niveau des points critiques de son infrastructure informatique, afin de protéger l'environnement du réseau.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(a)	a) Le service BFI doit installer des dispositifs de sécurité réseau, tels que des pare-feu, des logiciels antivirus et contre les programmes malveillants, ainsi que des systèmes de détection et de prévention des intrusions, au niveau des points critiques de son infrastructure informatique, afin de protéger l'environnement du réseau.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(a)	a) Le service BFI doit installer des dispositifs de sécurité réseau, tels que des pare-feu, des logiciels antivirus et contre les programmes malveillants, ainsi que des systèmes de détection et de prévention des intrusions, au niveau des points critiques de son infrastructure informatique, afin de protéger l'environnement du réseau.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informatiques si nécessaire - Des contrôles spécifiques doivent être réalisés pour préserver la confidentialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	opensearch-node-to -node-encryption-c heck	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informatiques si nécessaire - Des contrôles spécifiques doivent être réalisés pour préserver la confidentialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informatiques si nécessaire - Des contrôles spécifiques doivent être réalisés pour préserver la confidentialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	ec2-instance-no-pu blic-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	internet-gateway-a uthorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectée s qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiel lement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informatiques si nécessaire - Des contrôles spécifiques doivent être réalisés pour préserver la confidentialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		Lambda doivent être attribuées à un VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	s3-bucket-public-w rite-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informatiques si nécessaire - Des contrôles spécifiques doivent être réalisés pour préserver la confidentialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	autoscaling-launch -config-public-ip- disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référenti els de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionn alités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informatiques si nécessaire - Des contrôles spécifiques doivent être réalisés pour préserver la confidentialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(c)	c) Des contrôles doivent être mis en œuvre pour garantir la sécurité des informations dans les réseaux ainsi que la protection des services connectés contre tout accès non autorisé. Les points suivants doivent particulièrement être pris en compte : - Les responsabilités et les procédures de gestion des équipements du réseau doivent être définies - La responsabilité opérationnelle des réseaux doit être séparée des opérations informati ques si nécessair e - Des contrôles spécifiques doivent être réalisés pour préserver la confident ialité et l'intégrité des données transitant via les réseaux publics ou les réseaux sans fil, et pour protéger les	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	systèmes et applications connectés (y compris les protocoles de chiffrement réseau lors de la connexion à des systèmes/réseaux non sécurisés). - Une journalisation et une surveillance appropriées doivent être réalisées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées - Les activités de gestion doivent être étroitement coordonnées à la fois pour optimiser le service de l'organisation et pour garantir que les contrôles sont appliqués de manière cohérente sur l'ensemble de l'infrastructure de traitement de l'information - Les systèmes du réseau doivent être authentifiés - Les connexions non		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	sécurisées au réseau doivent être limitées		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionnalités de sécurité des services réseau doivent comprendre les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authentification, le chiffrement et les contrôles de connexion au réseau - Des paramètres techniques obligatoires pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionn alités de sécurité des services réseau doivent comprendr e les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authent ification, le chiffreme nt et les contrôles de connexion au réseau - Des paramètres techniques obligatoi res pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionnalités de sécurité des services réseau doivent comprendre les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authentification, le chiffrement et les contrôles de connexion au réseau - Des paramètres techniques obligatoires pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionnalités de sécurité des services réseau doivent comprendre les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authentification, le chiffrement et les contrôles de connexion au réseau - Des paramètres techniques obligatoires pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionnalités de sécurité des services réseau doivent comprendre les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authentification, le chiffrement et les contrôles de connexion au réseau - Des paramètres techniques obligatoires pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionn alités de sécurité des services réseau doivent comprendr e les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authent ification, le chiffreme nt et les contrôles de connexion au réseau - Des paramètres techniques obligatoi res pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionn alités de sécurité des services réseau doivent comprendr e les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authent ification, le chiffreme nt et les contrôles de connexion au réseau - Des paramètres techniques obligatoi res pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionnalités de sécurité des services réseau doivent comprendre les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authentification, le chiffrement et les contrôles de connexion au réseau - Des paramètres techniques obligatoires pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionn alités de sécurité des services réseau doivent comprendr e les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authent ification, le chiffreme nt et les contrôles de connexion au réseau - Des paramètres techniques obligatoi res pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionn alités de sécurité des services réseau doivent comprendr e les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authent ification, le chiffreme nt et les contrôles de connexion au réseau - Des paramètres techniques obligatoi res pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2(e)	e) Les services réseau peuvent aller d'une simple bande passante non gérée à des services sophistiqués tels qu'un VPN, VoIP (voix sur IP), VSAT, etc. Les fonctionnalités de sécurité des services réseau doivent comprendre les éléments suivants : - Une technologie appliquée à la sécurité des services réseau telle que l'authentification, le chiffrement et les contrôles de connexion au réseau - Des paramètres techniques obligatoires pour garantir une connexion sécurisée aux services réseau conformément aux règles de sécurité et de connexion au réseau - Des procédures liées à l'utilisation des services réseau afin	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de restreindre l'accès aux services ou applications réseau, si nécessaire		
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
3.1.3(e)	e) Utilisez le chiffrement pour protéger les canaux de communication entre l'appareil permettant l'accès à distance et l'établissement afin de limiter les risques d'usurpation réseau.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(g)	g) Générez des journaux regroupant les communications avec accès à distance. Ces journaux doivent inclure la date, l'heure, l'utilisateur, l'emplacement de l'utilisateur, la durée et le but de tout accès à distance, y compris toutes les activités réalisées via un accès à distance	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(i)	i) Appliquer un processus d'authentification à deux facteurs pour l'accès à distance (par exemple, carte à jeton basée sur un code PIN avec un générateur de mot de passe aléatoire à usage unique, ou PKI basée sur un jeton)	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(i)	i) Appliquer un processus d'authent ification à deux facteurs pour l'accès à distance (par exemple, carte à jeton basée sur un code PIN avec un générateur de mot de passe aléatoire à usage unique, ou PKI basée sur un jeton)	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(i)	i) Appliquer un processus d'authentification à deux facteurs pour l'accès à distance (par exemple, carte à jeton basée sur un code PIN avec un générateur de mot de passe aléatoire à usage unique, ou PKI basée sur un jeton)	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3(i)	i) Appliquer un processus d'authentification à deux facteurs pour l'accès à distance (par exemple, carte à jeton basée sur un code PIN avec un générateur de mot de passe aléatoire à usage unique, ou PKI basée sur un jeton)	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(c)(e)	c) Le processus de gestion des correctifs doit inclure des aspects tels que : - Déterminer les méthodes d'obtention et de validation des correctifs afin de garantir que le correctif provient d'une source autorisée - Identifier les vulnérabilités applicables aux applications et aux systèmes utilisés par l'organisation - Évaluation de l'impact commercial de l'implémentation des correctifs (ou de la non-mise en œuvre d'un correctif en particulier) - Garantie des tests des correctifs - Description des méthodes de déploiement des correctifs, par exemple automatiquement - Rapport sur l'état du déploiement des correctifs au sein	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de l'organisation et - Y compris les méthodes pour faire face à l'échec du déploiement d'un correctif (par exemple, le redéploiement du correctif). e) Les BFI devraient déployer des outils de gestion automatique des correctifs et des outils de mise à jour logicielle pour tous les systèmes pour lesquels ces outils sont disponibles et sûrs		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(c)(e)	c) Le processus de gestion des correctif s doit inclure des aspects tels que : - Déterminer les méthodes d'obtenti on et de validatio n des correctifs afin de garantir que le correctif provient d'une source autorisée - Identifie r les vulnérabilités applicables aux applications et aux systèmes utilisés par l'organisation - Évaluation de l'impact commercia l de l'implémentation des correctifs (ou de la non-mise en œuvre d'un correctif en particulier) - Garantie des tests des correctif s - Description des méthodes de déploiement des correctifs, par exemple automatiq uement - Rapport sur l'état du déploiement des correctifs au sein	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de l'organisation et - Y compris les méthodes pour faire face à l'échec du déploiement d'un correctif (par exemple, le redéploiement du correctif). e) Les BFI devraient déployer des outils de gestion automatique des correctifs et des outils de mise à jour logicielle pour tous les systèmes pour lesquels ces outils sont disponibles et sûrs		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(c)(e)	c) Le processus de gestion des correctif s doit inclure des aspects tels que : - Déterminer les méthodes d'obtenti on et de validatio n des correctifs afin de garantir que le correctif provient d'une source autorisée - Identifie r les vulnérabilités applicables aux applications et aux systèmes utilisés par l'organisation - Évaluation de l'impact commercia l de l'implémentation des correctifs (ou de la non-mise en œuvre d'un correctif en particulier) - Garantie des tests des correctif s - Description des méthodes de déploiement des correctifs, par exemple automatiq uement - Rapport sur l'état du déploiement des correctifs au sein	ec2-managedinstanc e-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de l'organisation et - Y compris les méthodes pour faire face à l'échec du déploiement d'un correctif (par exemple, le redéploiement du correctif). e) Les BFI devraient déployer des outils de gestion automatique des correctifs et des outils de mise à jour logicielle pour tous les systèmes pour lesquels ces outils sont disponibles et sûrs		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(c)(e)	c) Le processus de gestion des correctifs doit inclure des aspects tels que : - Déterminer les méthodes d'obtention et de validation des correctifs afin de garantir que le correctif provient d'une source autorisée - Identifier les vulnérabilités applicables aux applications et aux systèmes utilisés par l'organisation - Évaluation de l'impact commercial de l'implémentation des correctifs (ou de la non-mise en œuvre d'un correctif en particulier) - Garantie des tests des correctifs - Description des méthodes de déploiement des correctifs, par exemple automatiquement - Rapport sur l'état du déploiement des correctifs au sein	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de l'organisation et - Y compris les méthodes pour faire face à l'échec du déploiement d'un correctif (par exemple, le redéploiement du correctif). e) Les BFI devraient déployer des outils de gestion automatique des correctifs et des outils de mise à jour logicielle pour tous les systèmes pour lesquels ces outils sont disponibles et sûrs		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(c)(e)	c) Le processus de gestion des correctif s doit inclure des aspects tels que : - Déterminer les méthodes d'obtenti on et de validatio n des correctifs afin de garantir que le correctif provient d'une source autorisée - Identifie r les vulnérabilités applicables aux applications et aux systèmes utilisés par l'organisation - Évaluation de l'impact commercia l de l'implémentation des correctifs (ou de la non-mise en œuvre d'un correctif en particulier) - Garantie des tests des correctif s - Description des méthodes de déploiement des correctifs, par exemple automatiq uement - Rapport sur l'état du déploiement des correctifs au sein	elastic-beanstalk-managed-updates-en abled	L'activation des mises à jour de plateforme gérées pour un environne ment Amazon Elastic Beanstalk garantit l'installation des derniers correctif s, mises à jour et fonctionnalités de la plateforme disponibl es pour l'environ nement. La sécurisat ion des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de l'organisation et - Y compris les méthodes pour faire face à l'échec du déploiement d'un correctif (par exemple, le redéploiement du correctif). e) Les BFI devraient déployer des outils de gestion automatique des correctifs et des outils de mise à jour logicielle pour tous les systèmes pour lesquels ces outils sont disponibles et sûrs		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(c)(e)	c) Le processus de gestion des correctif s doit inclure des aspects tels que : - Déterminer les méthodes d'obtenti on et de validatio n des correctifs afin de garantir que le correctif provient d'une source autorisée - Identifie r les vulnérabilités applicables aux applications et aux systèmes utilisés par l'organisation - Évaluation de l'impact commercia l de l'implémentation des correctifs (ou de la non-mise en œuvre d'un correctif en particulier) - Garantie des tests des correctif s - Description des méthodes de déploiement des correctifs, par exemple automatiq uement - Rapport sur l'état du déploiement des correctifs au sein	rds-automatic-mino r-version-upgrade-enabled	Activez les mises à niveau automatiq ues des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationn elle (RDBMS) sont installées, lesquelle s peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de l'organisation et - Y compris les méthodes pour faire face à l'échec du déploiement d'un correctif (par exemple, le redéploiement du correctif). e) Les BFI devraient déployer des outils de gestion automatique des correctifs et des outils de mise à jour logicielle pour tous les systèmes pour lesquels ces outils sont disponibles et sûrs		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(d)(e)	d) Une gestion appropriée des clés implique des processus sécurisés pour générer, stocker, archiver, récupérer , distribuer, retirer et supprimer les clés cryptographiques e) Toutes les clés cryptographiques doivent être protégées contre toute modificat ion ou perte. En outre, les clés secrètes et privées doivent être protégées contre toute utilisati on ou divulgation non autorisées. L'équipement utilisé pour générer, stocker et archiver les clés doit être protégé physiquement	kms-cmk-not-schedu led-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(d)(e)	d) Une gestion appropriée des clés implique des processus sécurisés pour générer, stocker, archiver, récupérer , distribuer, retirer et supprimer les clés cryptographiques e) Toutes les clés cryptographiques doivent être protégées contre toute modificat ion ou perte. En outre, les clés secrètes et privées doivent être protégées contre toute utilisati on ou divulgation non autorisées. L'équipement utilisé pour générer, stocker et archiver les clés doit être protégé physiquement	cmk-backing-key-ro tation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(d)(e)	d) Une gestion appropriée des clés implique des processus sécurisés pour générer, stocker, archiver, récupérer , distribuer, retirer et supprimer les clés cryptographiques e) Toutes les clés cryptographiques doivent être protégées contre toute modificat ion ou perte. En outre, les clés secrètes et privées doivent être protégées contre toute utilisati on ou divulgation non autorisées. L'équipement utilisé pour générer, stocker et archiver les clés doit être protégé physiquement	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4(d)(e)	d) Une gestion appropriée des clés implique des processus sécurisés pour générer, stocker, archiver, récupérer , distribuer, retirer et supprimer les clés cryptographiques e) Toutes les clés cryptographiques doivent être protégées contre toute modificat ion ou perte. En outre, les clés secrètes et privées doivent être protégées contre toute utilisati on ou divulgation non autorisées. L'équipement utilisé pour générer, stocker et archiver les clés doit être protégé physiquement	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5(f)	f) Un système de gestion des clés doit être basé sur un ensemble convenu de normes, de procédures et de méthodes sécurisées pour : - générer des clés pour différents systèmes cryptographiques et différentes applications - délivrer et obtenir des certificats de clé publique - distribuer des clés aux entités visées, y compris la manière dont les clés doivent être activées lors de leur réception - stocker les clés, y compris la manière dont les clés doivent être modifiées et comment cela sera fait - traiter les clés compromises - révoquer les clés y compris les clés doit être retiré ou désactivé, par exemple lorsque des clés ont été	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	compromises ou lorsqu'un utilisateur quitte une organisat ion (auquel cas les clés doivent également être archivées), pour récupérer des clés perdues ou corrompues, pour sauvegarder ou archiver des clés, pour détruire des clés et pour enregistrer et auditer les activités liées à la gestion des clés.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5(f)	f) Un système de gestion des clés doit être basé sur un ensemble convenu de normes, de procédures et de méthodes sécurisées pour : - générer des clés pour différents systèmes cryptographiques et différentes applications - délivrer et obtenir des certificats de clé publique - distribuer des clés aux entités visées, y compris la manière dont les clés doivent être activées lors de leur réception - stocker les clés, y compris la manière dont les clés doivent être modifiées et comment cela sera fait - traiter les clés compromises - révoquer les clés y compris les clés doit être retiré ou désactivé, par exemple lorsque des clés ont été	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	compromises ou lorsqu'un utilisateur quitte une organisat ion (auquel cas les clés doivent également être archivées), pour récupérer des clés perdues ou corrompues, pour sauvegarder ou archiver des clés, pour détruire des clés et pour enregistrer et auditer les activités liées à la gestion des clés.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5(f)	f) Un système de gestion des clés doit être basé sur un ensemble convenu de normes, de procédures et de méthodes sécurisées pour : - générer des clés pour différents systèmes cryptographiques et différentes applications - délivrer et obtenir des certificats de clé publique - distribuer des clés aux entités visées, y compris la manière dont les clés doivent être activées lors de leur réception - stocker les clés, y compris la manière dont les clés doivent être modifiées et comment cela sera fait - traiter les clés compromises - révoquer les clés y compris les clés doit être retiré ou désactivé, par exemple lorsque des clés ont été	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	compromises ou lorsqu'un utilisateur quitte une organisat ion (auquel cas les clés doivent également être archivées), pour récupérer des clés perdues ou corrompues, pour sauvegarder ou archiver des clés, pour détruire des clés et pour enregistrer et auditer les activités liées à la gestion des clés.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5(f)	f) Un système de gestion des clés doit être basé sur un ensemble convenu de normes, de procédures et de méthodes sécurisées pour : - générer des clés pour différents systèmes cryptographiques et différentes applications - délivrer et obtenir des certificats de clé publique - distribuer des clés aux entités visées, y compris la manière dont les clés doivent être activées lors de leur réception - stocker les clés, y compris la manière dont les clés doivent être modifiées et comment cela sera fait - traiter les clés compromises - révoquer les clés y compris les clés doit être retiré ou désactivé, par exemple lorsque des clés ont été	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	compromises ou lorsqu'un utilisateur quitte une organisat ion (auquel cas les clés doivent également être archivées), pour récupérer des clés perdues ou corrompues, pour sauvegarder ou archiver des clés, pour détruire des clés et pour enregistrer et auditer les activités liées à la gestion des clés.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5(f)	f) Un système de gestion des clés doit être basé sur un ensemble convenu de normes, de procédures et de méthodes sécurisées pour : - générer des clés pour différents systèmes cryptographiques et différentes applications - délivrer et obtenir des certificats de clé publique - distribuer des clés aux entités visées, y compris comment les clés doivent être activées lors de leur réception - stocker les clés, y compris la manière dont les clés doivent être modifiées et comment cela sera fait - traiter les clés compromises - révoquer les clés y compris les clés doit être retiré ou désactivé, par exemple lorsque des clés ont été compromises ou	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	lorsqu'un utilisateur quitte une organisat ion (auquel cas les clés doivent également être archivées), pour récupérer des clés perdues ou corrompues, pour sauvegarder ou archiver des clés, pour détruire des clés et pour enregistrer et auditer les activités liées à la gestion des clés.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5(f)	f) Un système de gestion des clés doit être basé sur un ensemble convenu de normes, de procédures et de méthodes sécurisées pour : - générer des clés pour différents systèmes cryptographiques et différentes applications - délivrer et obtenir des certificats de clé publique - distribuer des clés aux entités visées, y compris comment les clés doivent être activées lors de leur réception - stocker les clés, y compris la manière dont les clés doivent être modifiées et comment cela sera fait - traiter les clés compromises - révoquer les clés y compris les clés doit être retiré ou désactivé, par exemple lorsque des clés ont été compromises ou	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	lorsqu'un utilisateur quitte une organisat ion (auquel cas les clés doivent également être archivées), pour récupérer des clés perdues ou corrompues, pour sauvegarder ou archiver des clés, pour détruire des clés et pour enregistrer et auditer les activités liées à la gestion des clés.		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5(f)	f) Un système de gestion des clés doit être basé sur un ensemble convenu de normes, de procédure s et de méthodes sécurisées pour : - générer des clés pour différents systèmes cryptographiques et différentes applicati ons - délivrer et obtenir des certifica ts de clé publique - distribuer des clés aux entités visées, y compris comment les clés doivent être activées lors de leur réception - stocker les clés, y compris la manière dont les clés doivent être modifiées et comment cela sera fait - traiter les clés compromis es - révoquer les clés y compris les clés doit être retiré ou désactivé, par exemple lorsque des clés ont été compromises ou	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	lorsqu'un utilisateur quitte une organisat ion (auquel cas les clés doivent également être archivées), pour récupérer des clés perdues ou corrompues, pour sauvegarder ou archiver des clés, pour détruire des clés et pour enregistrer et auditer les activités liées à la gestion des clés.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.6(a)	a) Le service BFI doit déployer une combinaison d'outils automatisés et de techniques manuelles pour effectuer périodiquement un test de vulnérabilité complet. Pour les systèmes Web externes, le champ d'application du test de vulnérabilité doit inclure les vulnérabilités Web courantes telles que l'injection SQL et les scripts inter-sites.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.6(a)	a) Le service BFI doit déployer une combinaison d'outils automatisés et de techniques manuelles pour effectuer périodiquement un test de vulnérabilité complet. Pour les systèmes Web externes, le champ d'application du test de vulnérabilité doit inclure les vulnérabilités Web courantes telles que l'injection SQL et les scripts inter-sites.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.6(a)	a) Le service BFI doit déployer une combinaison d'outils automatisés et de techniques manuelles pour effectuer périodiquement un test de vulnérabilité complet. Pour les systèmes Web externes, le champ d'application du test de vulnérabilité doit inclure les vulnérabilités Web courantes telles que l'injection SQL et les scripts inter-sites.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.6(c)	c) Le service BFI doit définir un processus pour remédier aux problèmes identifiés au cours des tests de vulnérabilité et d'intrusion, et revérifier ultérieurement la correction appliquée pour s'assurer que les lacunes sont entièrement corrigées.	vuln-mitigated-accepted(vérification du processus)	Assurez-vous que les vulnérabilités nouvellement identifiées sont corrigées ou documentées en tant que risques acceptés. Les vulnérabilités doivent être corrigées ou considérées comme des risques conformément aux exigences de conformité de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.6(f)	f) La fonction de sécurité doit fournir des données actualisées sur le nombre de vulnérabilités critiques non atténuées pour chaque département/service, et un plan d'atténuation aux cadres supérieures à intervalles réguliers	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.8	Formation et sensibilisation des utilisateurs	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.10(b)	b) Les informations sensibles telles que la documentation du système, le code source de l'application et les données des transactions de production devraient faire l'objet de contrôles plus étendus pour éviter toute modification (par exemple, vérificateurs d'intégrité, hachages cryptographiques). En outre, les politiques établies doivent minimiser la diffusion d'informations sensibles, y compris les impressions contenant ces informations.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(h)	h) Afin de minimiser les risques associés aux modifications, les services BFI doivent sauvegarder les systèmes ou applications concernés avant toute modification. Si un problème survient pendant ou après le déploiement, les services BFI doivent définir un plan de restauration pour revenir à une ancienne version du système ou de l'application.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informati ons utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalis ation est prêt à enregistrer les activités réalisées pendant le processus de migration.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1(k)	k) Les journaux d'audit et de sécurité sont des informations utiles qui faciliten t les enquêtes et le dépannage. Le service BFI doit s'assurer que le système de journalisation est prêt à enregistrer les activités réalisées pendant le processus de migration.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.3(a)	a) Développez et mettez en œuvre des processus de prévention, de détection, d'analyse et de réponse aux incidents de sécurité des informations.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.3(a)	a) Développez et mettez en œuvre des processus de prévention, de détection, d'analyse et de réponse aux incidents de sécurité des informations.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibi lité du système, une capacité approprié e, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibi lité du système, une capacité approprié e, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibi lité du système, une capacité approprié e, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibi lité du système, une capacité approprié e, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibilité du système, une capacité appropriée, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
3.3.1(a)	a) Tenez compte des facteurs importants permettant de garantir une haute disponibi lité du système, une capacité approprié e, des performances fiables, un temps de réponse rapide et une capacité de mise à l'échelle dans le cadre de la conception du système.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisate urs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalis ation des audits des activités du système réalisées par les utilisateurs privilégi és. f) Garantissez une journalisation et une surveillance approprié es pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées . j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatis és capables de	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisate urs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalis ation des audits des activités du système réalisées par les utilisateurs privilégi és. f) Garantissez une journalisation et une surveillance approprié es pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées . j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatis és capables de	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisate urs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalis ation des audits des activités du système réalisées par les utilisateurs privilégi és. f) Garantissez une journalisation et une surveillance approprié es pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées . j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatis és capables de	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisate urs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalis ation des audits des activités du système réalisées par les utilisateurs privilégi és. f) Garantissez une journalisation et une surveillance approprié es pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées . j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatis és capables de	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(a)(b)(c)(f)(j)	a) Veillez à ce que les enregistrements des accès des utilisateurs soient identifiés et journalisés de façon unique à des fins d'audit et de révision. b) Documentez la responsabilité et l'identification des accès non autorisés. c) Activez la journalisation des audits des activités du système réalisées par les utilisateurs privilégiés. f) Garantissez une journalisation et une surveillance appropriées pour permettre l'enregistrement et la détection des actions susceptibles d'affecter la sécurité des informations, ou qui y sont associées. j) Assurez-vous que la journalisation des événements constitue la base des systèmes de surveillance automatisés capables de	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	générer des rapports consolidés et des alertes sur la sécurité du système.		
3.4(f)	f) Veillez à effectuer une journalisation et une surveillance appropriées pour permettre l'enregis trement et la détection des actions susceptib les d'affecter la sécurité des informati ons, ou qui y sont associées.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4(g)	g) Assurez-vous que les journaux d'événements incluent, le cas échéant : - Les identifiants des utilisateurs - Les activités du système - Les dates, heures et détails des événements clés, par exemple la connexion et la déconnexion - L'identité ou l'emplacement de l'appareil si possible et l'identifiant du système - Enregistrements des tentatives d'accès au système réussies et rejetées - Enregistrements des tentatives d'accès aux données et autres ressources - Modifications de la configuration du système - Utilisation des utilitaires et applications du système - Fichiers consultés et type d'accès - Adresses et protocoles réseau	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	- Alarmes soulevée par le système de contrôle d'accès et - Enregistrements des transactions exécutées par les utilisateurs dans les applications et les transactions clients en ligne		
3.6.1(a)(h)	a) Les services BFI doivent garantir des mesures de sécurité appropriées pour leurs applications Web et prendre les mesures d'atténuation adéquates contre les divers risques liés à la sécurité Web. h) Les services BFI doivent garantir des mesures de sécurité approprié es pour leurs applicati ons Web et prendre les mesures d'atténua tion adéquates contre les divers risques liés à la sécurité Web	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(a)(h)	a) Les services BFI doivent garantir des mesures de sécurité appropriées pour leurs applications Web et prendre les mesures d'atténuation adéquates contre les divers risques liés à la sécurité Web. h) Les services BFI doivent garantir des mesures de sécurité approprié es pour leurs applicati ons Web et prendre les mesures d'atténua tion adéquates contre les divers risques liés à la sécurité Web	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
3.6.1(b)	b) Les BFI doivent évaluer les exigences de sécurité associées à leurs systèmes bancaires en ligne et aux autres systèmes concernés, et adopter une solution de chiffrement tenant compte du degré de confidentialité et d'intégrité requis.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(d)	d) Les BFI proposant des services bancaires en ligne doivent immédiate ment réagir en cas de trafic réseau/ de performances système inhabitue ls, et d'augmentation soudaine de l'utilisa tion des ressource s du système, ce qui pourrait indiquer une attaque DDoS. Par conséquent, le succès de toute action préventive et réactive dépend du déploiement d'outils appropriés pour détecter, surveiller et analyser efficacem ent les anomalies des réseaux et des systèmes.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(d)	d) Les BFI proposant des services bancaires en ligne doivent immédiatement réagir en cas de trafic réseau/de performances système inhabituels, et d'augmentation soudaine de l'utilisation des ressources du système, ce qui pourrait indiquer une attaque DDoS. Par conséquent, le succès de toute action préventive et réactive dépend du déploiement d'outils appropriés pour détecter, surveiller et analyser efficacement les anomalies des réseaux et des systèmes.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveiller et à détecter les événements de cybersécurité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(d)	d) Les BFI proposant des services bancaires en ligne doivent immédiate ment réagir en cas de trafic réseau/ de performances système inhabitue ls, et d'augmentation soudaine de l'utilisa tion des ressource s du système, ce qui pourrait indiquer une attaque DDoS. Par conséquent, le succès de toute action préventive et réactive dépend du déploiement d'outils appropriés pour détecter, surveiller et analyser efficacem ent les anomalies des réseaux et des systèmes.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(d)	d) Les BFI proposant des services bancaires en ligne doivent immédiatement réagir en cas de trafic réseau/de performances système inhabituels, et d'augmentation soudaine de l'utilisation des ressources du système, ce qui pourrait indiquer une attaque DDoS. Par conséquent, le succès de toute action préventive et réactive dépend du déploiement d'outils appropriés pour détecter, surveiller et analyser efficacement les anomalies des réseaux et des systèmes.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(d)	d) Les BFI proposant des services bancaires en ligne doivent immédiatement réagir en cas de trafic réseau/de performances système inhabituels, et d'augmentation soudaine de l'utilisation des ressources du système, ce qui pourrait indiquer une attaque DDoS. Par conséquent, le succès de toute action préventive et réactive dépend du déploiement d'outils appropriés pour détecter, surveiller et analyser efficacement les anomalies des réseaux et des systèmes.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1(e)	e) Les BFI doivent évaluer régulièrement les vulnérabilités en matière de sécurité des informations ainsi que l'efficacité du framework de gestion des risques de sécurité informatiques existant en apportant les ajustements nécessaires, afin que les vulnérabilités émergentes soient traitées en temps opportun. Cette évaluation doit également être réalisée en cas de modification importante.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.4(a)(b)	a) Limitez l'accès à Internet et séparez les systèmes critiques de l'environnement informatique général. b) Réduisez la surface d'attaque et les vulnérabilités.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NBC TRMG.

Bonnes pratiques de fonctionnement pour NERC CIP BCSI

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les normes de protection des infrastructures critiques (NERC CIP) de la North American Electric Reliability Corporation pour les informations sur les cybersystèmes BES (BCSI), CIP-004-7 et CIP-011-3, et les règles gérées. AWS Config Chaque règle de AWS configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NERC CIP applicables au BCSI. Un contrôle NERC CIP peut être associé à

plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des OpenSearch tableaux de bord mutualisés et l'authentification HTTP de base pour Kibana et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	L'accès accordé doit être considéré comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		que d'autres informati ons administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-004-7-R6-Partie 6.1	Chaque entité responsable doit mettre en place un ou plusieurs programmes de gestion des accès documentés pour autoriser, vérifier et révoquer l'accès accordé au BCSI relatif aux « systèmes applicables » identifiés dans le tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information), qui incluent collectivement chacune des parties des exigences applicables du tableau R6 du CIP-004-7 (Access Management for BES Cyber System Information). Pour obtenir l'accès au BCSI dans le cadre de cette exigence, une personne peut à la fois obtenir et utiliser le BCSI. L'accès accordé doit être considéré	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	comme le résultat des mesures spécifiqu es prises pour fournir à une ou plusieurs personnes les moyens d'accéder au BCSI (par exemple, cela peut inclure des clés physiques ou des cartes d'accès, des utilisateurs et des droits et privilèges associés, des clés de chiffrement). Partie 6.1 : avant de fournir un accès à un utilisateur, autorisez -le (sauf si déjà autorisé conformém ent à la partie 4.1.) à y accéder selon ses besoins, conformém ent à la notion d'entité responsable, excepté en cas de circonsta nces exceptionnelles du CIP : 6.1.1. Fournir un accès électronique au BCSI électronique		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	ecr-private-tag-immutability-enabled	Activez l'immuabilité des balises Elastic Container Repository (ECR) pour éviter que les balises de vos images ECR ne soient écrasées. Jusqu'à présent, les balises pouvaient être écrasées, ce qui nécessitait l'utilisation de méthodes manuelles pour identifier une image de manière unique.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que les clés principales du client (CMK) nécessaires ne sont pas programmées pour être supprimées dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	s3-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	rds-cluster-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut contribuer à réduire la surface d'attaque de votre ou de vos clusters de base de données Amazon Relational Database Service (Amazon RDS).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	rds-instance-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut contribuer à réduire la surface d'attaque de votre ou de vos instances de base de données Amazon Relational Database Service (Amazon RDS).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	redshift-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut réduire la surface d'attaque de votre ou de vos clusters Amazon Redshift.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CIP-011-3-R1-Partie 1.2	Chaque entité responsable doit mettre en place un ou plusieurs programmes de protection des informations documentés qui incluent collectivement chacune des parties des exigences applicables du tableau R1 du CIP-011-3 (Information Protection). Partie 1.2 : les méthodes à utiliser pour protéger et gérer de manière sécurisée le BCSI afin d'atténuer les risques en termes de confidentialité.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NERC CIP BCSI.

Bonnes pratiques de fonctionnement pour les principes de sécurité du cloud NCSC

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les principes de sécurité du cloud du National Cyber Security Centre (NCSC) du Royaume-Uni et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles du NCSC Cloud Security Principles du Royaume-Uni. Un contrôle des principes de sécurité du cloud NCSC du Royaume-Uni peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages avec des contrôles au sein des principes de sécurité du cloud NCSC du Royaume-Uni (National Cyber Security Centre | Cloud security guidance). Ces informations du secteur public sont sous licence Open Government Licence v3.0. La licence Open Government Licence peut être consultée ici : Licence Open Government Licence pour les informations du secteur public

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	acm-certificate-ex piration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	opensearch-https-r equired	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	opensearch-node-to -node-encryption-c heck	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1. Protection des données en transit	Les réseaux sur lesquels transiten t les données des utilisateurs doivent être protégés de manière adéquate contre la falsification et l'écoute clandesti ne.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2. Protection et résilience des actifs	Vos données (et les actifs qui les stockent ou les traitent) doivent être protégées de manière adéquate.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opération nelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
5. Sécurité opérationnelle	Les services doivent être exploités et gérés de manière à empêcher, détecter ou anticiper les attaques.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7. Développement sécurisé	Les services cloud doivent être conçus, développés et déployés de manière à limiter et atténuer les menaces qui menacent leur sécurité.	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7. Développement sécurisé	Les services cloud doivent être conçus, développés et déployés de manière à limiter et atténuer les menaces qui menacent leur sécurité.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7. Développement sécurisé	Les services cloud doivent être conçus, développés et déployés de manière à limiter et atténuer les menaces qui menacent leur sécurité.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codebuild . Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
9. Gestion des utilisateurs sécurisée	Les fournisseurs doivent proposer des outils vous permettant d'utiliser leurs services en toute sécurité.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	rds-instance-iam-authentication-enabled	Assurez-vous qu'une authentification AWS Identity and Access Management (IAM) est activée sur les instances Amazon Relational Database Service (Amazon RDS) afin de contrôler l'accès aux systèmes et aux actifs. Cela permet de chiffrer le trafic réseau à destination et en provenance de la base de données au moyen du protocole SSL. Il n'est pas nécessaire de stocker des informations d'identification utilisateur dans la base de données, car l'authentification est gérée de manière externe.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interface s de service doit être limité aux personnes authentifiées et autorisées.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interface s de service doit être limité aux personnes authentifiées et autorisées.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10. Identité et authentification	L'accès aux interfaces de service doit être limité aux personnes authentifiées et autorisées.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	ecs-container-insights-enabled	La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Elastic Container Service (ECS) et de vos AWS solutions. Conteneur Insights fournit également des informations de diagnostic (par exemple sur les échecs de redémarrage des conteneurs) pour vous aider à isoler les problèmes et à les résoudre rapidement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interfaces externes ou moins sécurisées du service doivent être identifiées et protégées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11. Protection des interfaces externes	Toutes les interface s externes ou moins sécurisées du service doivent être identifié es et protégées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
12. Administration sécurisée des services	Les fournisseurs de cloud doivent se rendre compte de la haute importance des systèmes d'adminis tration.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13. Informations d'audit pour les utilisateurs	Les fournisseurs doivent fournir les journaux nécessaires pour surveiller l'accès à votre service et aux données qu'il contient.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13. Informations d'audit pour les utilisateurs	Les fournisseurs doivent fournir les journaux nécessaires pour surveiller l'accès à votre service et aux données qu'il contient.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13. Informations d'audit pour les utilisateurs	Les fournisseurs doivent fournir les journaux nécessaires pour surveiller l'accès à votre service et aux données qu'il contient.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
13. Informations d'audit pour les utilisateurs	Les fournisseurs doivent fournir les journaux nécessaires pour surveiller l'accès à votre service et aux données qu'il contient.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les principes de sécurité du cloud du NCSC.

Bonnes pratiques de fonctionnement pour NCSC Cyber Assesment Framework

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les contrôles du cadre d'évaluation cybernétique (CAF) du National Cyber Security Centre (NCSC) du Royaume-Uni et les règles de AWS configuration gérées. Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NCSC CAF britanniques. Un contrôle UK NCSC CAF peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages avec des contrôles au sein du UK NCSC CAF (National Cyber Security Centre | NCSC CAF guidance). Ces informations du secteur public sont sous licence Open Government Licence v3.0. La licence Open Government Licence peut être consultée ici : Licence Open Government Licence pour les informations du secteur public

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
A3.a Gestion des actifs	Tous les éléments nécessaires pour fournir, entretenir ou soutenir des réseaux et des systèmes d'information afin de garantir le bon fonctionnement des fonctions essentiel les sont identifié s et compris. Cela inclut les données, les personnes et les systèmes, ainsi que toute infrastructure annexe (telle que l'alimentation ou le refroidissement).	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.
A3.a Gestion des actifs	Tous les éléments nécessaires pour fournir, entretenir ou	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	soutenir des réseaux et des systèmes d'information afin de garantir le bon fonctionnement des fonctions essentiel les sont identifié s et compris. Cela inclut les données, les personnes et les systèmes, ainsi que toute infrastructure annexe (telle que l'alimentation ou le refroidissement).		sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
A3.a Gestion des actifs	Tous les éléments nécessaires pour fournir, entretenir ou soutenir des réseaux et des systèmes d'information afin de garantir le bon fonctionnement des fonctions essentiel les sont identifié s et compris. Cela inclut les données, les personnes et les systèmes, ainsi que toute infrastructure annexe (telle que l'alimentation ou le refroidissement).	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
A3.a Gestion des actifs	Tous les éléments nécessaires pour fournir, entretenir ou soutenir des réseaux et des systèmes d'information afin de garantir le bon fonctionnement des fonctions essentiel les sont identifié s et compris. Cela inclut les données, les personnes et les systèmes, ainsi que toute infrastructure annexe (telle que l'alimentation ou le refroidissement).	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
A3.a Gestion des actifs	Tous les éléments nécessaires pour fournir, entretenir ou soutenir des réseaux et des systèmes d'information afin de garantir le bon fonctionnement des fonctions essentiel les sont identifié s et compris. Cela inclut les données, les personnes et les systèmes, ainsi que toute infrastructure annexe (telle que l'alimentation ou le refroidissement).	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentif ication et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'informa tion qui soutienne nt votre fonction essentielle.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentif ication et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'informa tion qui soutienne nt votre fonction essentielle.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentif ication et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'informa tion qui soutienne nt votre fonction essentielle.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentif ication et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'informa tion qui soutienne nt votre fonction essentielle.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentification et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentif ication et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'informa tion qui soutienne nt votre fonction essentielle.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearc h Service. Le contrôle d'accès précis fournit des mécanisme s d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authent ification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.a Vérification de l'identité, authentif ication et autorisation	Vous vérifiez, authentifiez et autorisez de manière fiable l'accès aux réseaux et aux systèmes d'informa tion qui soutienne nt votre fonction essentielle.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
B2.b Gestion des appareils	Vous connaissez parfaitement les appareils utilisés pour accéder à vos réseaux, à vos systèmes d'information et aux données qui soutiennent vos fonctions essentielles, et savez qu'il s'agit d'appareils sécurisés.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.b Gestion des appareils	Vous connaissez parfaitement les appareils utilisés pour accéder à vos réseaux, à vos systèmes d'information et aux données qui soutiennent vos fonctions essentielles, et savez qu'il s'agit d'appareils sécurisés.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.c Gestion des utilisateurs privilégiés	Vous gérez étroitement l'accès privilégié des utilisateurs aux réseaux et aux systèmes d'information qui soutiennent votre fonction essentielle.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B2.d Gestion des identités et des accès (IdAM)	Vous assurez la bonne gestion et la maintenance du contrôle de l'identité et des accès pour les réseaux et systèmes d'information soutenant votre fonction essentielle.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.a Compréhension des données	Vous comprenez parfaitement les données cruciales pour le fonctionnement de votre fonction essentielle, l'endroit où elles sont stockées, où elles se déplacent, et comment leur indisponibilité, ou un accès, une modification ou une suppression non autorisés pourraient avoir un impact négatif sur votre fonction essentielle. Cela vaut également pour les tiers qui stockent ou accèdent à des données importantes pour le fonctionnement de vos fonctions essentielles.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.b Données en transit	Vous avez protégé le transit des données qui est important pour le fonctionnement de votre fonction essentielle. Cela inclut le transfert de données à des tiers.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B3.c Données stockées	Vous avez protégé les données stockées importantes pour le fonctionnement de votre fonction essentielle.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploitation d'une seule vulnérabilité.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.a Sécurité intégrée à la conception	Vous intégrez la sécurité au réseau et aux systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles dès la conception. Vous minimisez leur surface d'attaque et vous vous assurez que le fonctionnement de votre fonction essentielle n'est pas affecté par l'exploit ation d'une seule vulnérabilité.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.b Configuration sécurisée	Vous configurez en toute sécurité le réseau et les systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.b Configuration sécurisée	Vous configurez en toute sécurité le réseau et les systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.b Configuration sécurisée	Vous configurez en toute sécurité le réseau et les systèmes d'informa tion qui garantissent le bon fonctionnement de vos fonctions essentielles.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.b Configuration sécurisée	Vous configurez en toute sécurité le réseau et les systèmes d'information qui garantissent le bon fonctionnement de vos fonctions essentielles.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.c Gestion sécurisée	Vous gérez le réseau et les systèmes d'information de votre organisation qui garantissent le bon fonctionnement de vos fonctions essentielles pour assurer et préserver la sécurité.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.c Gestion sécurisée	Vous gérez le réseau et les systèmes d'information de votre organisation qui garantissent le bon fonctionnement de vos fonctions essentielles pour assurer et préserver la sécurité.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.c Gestion sécurisée	Vous gérez le réseau et les systèmes d'information de votre organisation qui garantissent le bon fonctionnement de vos fonctions essentielles pour assurer et préserver la sécurité.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.d. Vulnerability Management	Vous gérez les vulnérabilités connues de votre réseau et de vos systèmes d'information afin d'éviter tout impact négatif sur vos fonctions essentiel les.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.d. Vulnerability Management	Vous gérez les vulnérabilités connues de votre réseau et de vos systèmes d'information afin d'éviter tout impact négatif sur vos fonctions essentiel les.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instanc e Amazon EC2 sont conformes dans AWS Systems Manager conformém ent aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.d. Vulnerability Management	Vous gérez les vulnérabilités connues de votre réseau et de vos systèmes d'information afin d'éviter tout impact négatif sur vos fonctions essentiel les.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.d. Vulnerability Management	Vous gérez les vulnérabilités connues de votre réseau et de vos systèmes d'information afin d'éviter tout impact négatif sur vos fonctions essentiel les.	redshift-cluster-m aintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisat ion. Plus préciséme nt, qu'ils disposent de fenêtres de maintenan ce préférées et de périodes de conservat ion des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrad e. Par défaut, la valeur est true. Il vous permet également de définir éventuell ement le preferred MaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotR etention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.d. Vulnerability Management	Vous gérez les vulnérabilités connues de votre réseau et de vos systèmes d'information afin d'éviter tout impact négatif sur vos fonctions essentiel les.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B4.d. Vulnerability Management	Vous gérez les vulnérabilités connues de votre réseau et de vos systèmes d'information afin d'éviter tout impact négatif sur vos fonctions essentiel les.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.b Conception axée sur la résilience	Vous concevez le réseau et les systèmes d'information qui garantissent le bon fonctionnement de votre fonction essentielle de manière à ce qu'ils soient résilients aux incidents de cybersécurité. Les systèmes sont correctement séparés et les limites de ressources sont atténuées.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.b Conception axée sur la résilience	Vous concevez le réseau et les systèmes d'informa tion qui garantiss ent le bon fonctionn ement de votre fonction essentiel le de manière à ce qu'ils soient résilient s aux incidents de cybersécurité. Les systèmes sont correctement séparés et les limites de ressources sont atténuées.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.b Conception axée sur la résilience	Vous concevez le réseau et les systèmes d'informa tion qui garantiss ent le bon fonctionn ement de votre fonction essentiel le de manière à ce qu'ils soient résilient s aux incidents de cybersécurité. Les systèmes sont correctement séparés et les limites de ressources sont atténuées.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
B5.c Sauvegardes	Vous possédez des sauvegardes actualisées, accessibles et sécurisées des données et informations nécessaires pour rétablir le bon fonctionnement de votre fonction essentielle	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identif ier rapidement les événements de sécurité susceptibles d'affecter le fonctionn ement de votre fonction essentielle.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identifier rapidement les événements de sécurité susceptibles d'affecter le fonctionnement de votre fonction essentielle.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identif ier rapidement les événements de sécurité susceptibles d'affecter le fonctionn ement de votre fonction essentielle.	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identif ier rapidement les événements de sécurité susceptibles d'affecter le fonctionn ement de votre fonction essentielle.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identif ier rapidement les événements de sécurité susceptibles d'affecter le fonctionn ement de votre fonction essentielle.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identifier rapidement les événements de sécurité susceptibles d'affecter le fonctionnement de votre fonction essentielle.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identif ier rapidement les événements de sécurité susceptibles d'affecter le fonctionn ement de votre fonction essentielle.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identif ier rapidement les événements de sécurité susceptibles d'affecter le fonctionn ement de votre fonction essentielle.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identifier rapidement les événements de sécurité susceptibles d'affecter le fonctionnement de votre fonction essentielle.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identif ier rapidement les événements de sécurité susceptibles d'affecter le fonctionn ement de votre fonction essentielle.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.a Couverture de surveillance	Les sources de données que vous incluez dans votre surveillance permettent d'identifier rapidement les événements de sécurité susceptibles d'affecter le fonctionnement de votre fonction essentielle.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfini e, elles seront alors supprimées.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfini e, elles seront alors supprimées.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfinie, elles seront alors supprimées.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.b Sécurisation des journaux	Vous conservez les données de journalisation en toute sécurité et n'accordez un accès en lecture qu'aux comptes devant obtenir cet accès pour des raisons professionnelles. Si aucun employé ne modifie ni supprime les données de journalisation pendant une période de conservation prédéfini e, elles seront alors supprimées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.c Déclenchement d'alertes	Les preuves d'incidents de sécurité potentiels contenues dans vos données de surveillance sont identifiées de manière fiable et déclenchent des alertes.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.d Identification des incidents de sécurité	Vous contextualisez les alertes en tenant compte de la menace et de vos systèmes, afin d'identifier les incidents de sécurité nécessitant une certaine forme de réponse.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.d Identification des incidents de sécurité	Vous contextualisez les alertes en tenant compte de la menace et de vos systèmes, afin d'identifier les incidents de sécurité nécessitant une certaine forme de réponse.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.e Outils et compétences liés à la surveillance	La surveillance des compétences, des outils et des rôles de la main-d'œuvre, y compris ceux qui sont externalisés, doit tenir compte des exigences en matière de gouvernance et de création de rapports, des menaces prévisionnelles, et de la complexité du réseau ou des données du système qu'il doit utiliser. La main-d'œuvre chargée de la surveillance connaît les fonctions essentielles qu'elle doit protéger.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.e Outils et compétences liés à la surveillance	La surveillance des compétences, des outils et des rôles de la main-d'œuvre, y compris ceux qui sont externalisés, doit tenir compte des exigences en matière de gouvernance et de création de rapports, des menaces prévisionnelles, et de la complexité du réseau ou des données du système qu'il doit utiliser. La main-d'œuvre chargée de la surveillance connaît les fonctions essentielles qu'elle doit protéger.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C1.e Outils et compétences liés à la surveillance	La surveillance des compétences, des outils et des rôles de la main-d'œuvre, y compris ceux qui sont externalisés, doit tenir compte des exigences en matière de gouvernance et de création de rapports, des menaces prévisionnelles, et de la complexité du réseau ou des données du système qu'il doit utiliser. La main-d'œuvre chargée de la surveillance connaît les fonctions essentielles qu'elle doit protéger.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C2.a Anomalies du système pour la détection des attaques	Vous définissez des exemples d'anomali es dans le comportem ent du système afin de créer des moyens pratiques de détecter des activités malveillantes difficiles à identifier d'une autre manière.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
C2.a Anomalies du système pour la détection des attaques	Vous définissez des exemples d'anomalies dans le comportement du système afin de créer des moyens pratiques de détecter des activités malveillantes difficiles à identifier d'une autre manière.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
D1.c Tests et exercices	Votre organisation effectue des exercices pour tester les plans de réponse en s'appuyant sur les incidents qui ont affecté votre organisation (et d'autres) dans le passé, et sur des scénarios tenant compte des renseignements sur les menaces et de votre évaluation des risques.	response-plan-exists-maintained (Vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiellement documentés permet de s'assurer que le personnel d'intervention comprend les rôles, les responsabilités et les processus à suivre en cas d'incident.
D1.c Tests et exercices	Votre organisation effectue des exercices pour tester les plans de réponse en s'appuyant sur les incidents qui ont affecté votre organisation (et d'autres) dans le passé, et sur des scénarios tenant compte des renseignements sur les menaces et de votre évaluation des risques.	response-plan-tested (Vérification du processus)	Assurez-vous que les plans de réponse et de reprise sont testés. Cela peut vous aider à comprendre si votre plan sera efficace en cas d'incident et si des lacunes doivent être corrigées ou des mises à jour effectuées.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NCSC Cyber Assessment Framework.

Bonnes pratiques de fonctionnement pour les services de mise en réseau et de diffusion de contenu

Ce pack de conformité contient des AWS Config règles basées sur les services de mise en réseau et de diffusion de contenu. Pour plus d'informations, consultez la section Mise en réseau et diffusion de contenu sur AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les services de mise en réseau et de diffusion de contenu.

Bonnes pratiques de fonctionnement pour NIST 800-53 rev 4

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le NIST 800-53 et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NIST 800-53. Un contrôle NIST 800-53 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Ce pack de conformité a été validé par AWS Security Assurance Services LLC (AWS SAS), qui est une équipe d'évaluateurs de sécurité qualifiés (QSA) dans le secteur des cartes de paiement, de praticiens certifiés par HITRUST Common Security Framework (CCSFP) et de professionnels de la conformité certifiés pour fournir des conseils et des évaluations pour divers frameworks industriels.

AWS Les professionnels de SAS ont conçu ce pack de conformité pour permettre à un client de s'aligner sur un sous-ensemble du NIST 800-53.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	secretsmanager-scheduled-rotation-success-vérifier	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC-2 (1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-user-group-membership-vérifier	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et le Centers for Internet Security (CIS) AWS Foundations Benchmark en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	iam-user-unused-credentials-vérifier	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(1)	L'organisation utilise des mécanismes automatisés pour faciliter la gestion des comptes du système d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(3)	Le système d'information désactive automatiquement les comptes inactifs après [Attribution : période définie par l'organisation].	iam-user-unused-credentials-vérifier	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de tous Régions AWS vers votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			sans avoir à faire quoi que ce soit.
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(4)	Le système d'information audite automatiquement les actions de création, de modification, d'activation, de désactivation et de suppression de comptes, et notifie [Attribution : personnel ou rôles définis par l'organisation].	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2 (12) (a)	L'organisation : a. Surveille les comptes du système d'informa tion pour [Attribution : utilisation atypique définie par l'organis ation].	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(12)(a)	L'organisation : a. Surveille les comptes du système d'information pour [Attribution : utilisation atypique définie par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	iam-user-unused-credentials-vérifier	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'information conformément à [Attribution : procédures ou conditions définies par l'organisation].	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et le Centers for Internet Security (CIS) AWS Foundations Benchmark en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(f)	L'organisation : f. Crée, active, modifie, désactive et supprime les comptes du système d'informa tion conformém ent à [Attribution : procédures ou conditions définies par l'organisation].	iam-root-access-key-vérifier	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	s3- bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2 (g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du Compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2 (g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
AC-2(g)	L'organisation : g. Surveille l'utilisation des comptes du système d'information.	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	secretsmanager-scheduled-rotation-success-vérifier	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2 (j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-user-group-membership-vérifier	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et le Centers for Internet Security (CIS) AWS Foundations Benchmark en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-root-access-key-vérifier	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformit é des comptes aux exigences de gestion des comptes [Attribut ion : fréquence définie par l'organisation].	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			que d'autres informations administratives sur chaque principal.
AC-2 (j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-group-has-users-vérifier	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-2(j)	L'organisation : j. Vérifie la conformité des comptes aux exigences de gestion des comptes [Attribution : fréquence définie par l'organisation].	iam-user-no-policies-vérifier	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-user-no-policies-vérifier	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-user-unused-credentials-vérifier	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	lambda-function-public-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	s3- bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-user-group-membership-vérifier	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-root-access-key-vérifier	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	ebs-snapshot-public-restorable-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			que d'autres informations administratives sur chaque principal.
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-group-has-users-vérifier	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-3	Le système d'information applique les autorisations approuvées pour l'accès logique aux informations et aux ressources du système conformément aux politiques de contrôle d'accès applicables.	sagemaker-notebook-no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	lambda-function-public-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	rds-instance-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			Lambda doivent être attribuées à un VPC.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	ec2- instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	sagemaker-notebook-no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	vpc-default-security-group-fermé	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	ebs-snapshot-public-restorable-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	emr-master-no-public-IP	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-4	Le système d'information applique les autorisations approuvées pour contrôler le flux d'informations au sein du système et entre les systèmes interconnectés conformément aux [Attribution : politiques de contrôle du flux d'informations définies par l'organisation].	internet-gateway-authorized-vpc-uniquement	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-5c	L'organisation : c. Définit les autorisat ions d'accès au système d'informa tion pour faciliter la séparation des tâches.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			que d'autres informations administratives sur chaque principal.
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-group-has-users-vérifier	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-5c	L'organisation : c. Définit les autorisations d'accès au système d'information pour faciliter la séparation des tâches.	iam-user-no-policies-vérifier	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	rds-instance-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	s3- bucket-policy-gran tee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_gran tee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principau x de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	s3- bucket-public-read -prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	s3- bucket-public-writ e-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	sagemaker-notebook -no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	lambda-function-pu blic-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	codebuild-project-envvar-awscred-vérifier	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild . AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	ebs-snapshot-public-restorable-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	iam-user-unused-cr edentials-vérifier	AWS Identity and Access Managemen t (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCreden tialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			que d'autres informations administratives sur chaque principal.
AC-6	L'organisation applique le principe du moindre privilège, en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-group-has-users-vérifier	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège, en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	iam-root-access-key-vérifier	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-user-group-membership-vérifier	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	iam-user-no-policies-vérifier	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organis ation et aux fonctions métier.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6	L'organisation applique le principe du moindre privilège , en n'accordant aux utilisateurs (ou aux processus agissant pour leur compte) que les accès autorisés nécessaires à l'accomplissement des tâches qui leur sont confiées, conformément aux missions de l'organisation et aux fonctions métier.	iam-no-inline-policy-vérifier	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-6 (10)	Le système d'information empêche les utilisateurs non privilégiés d'exécuter des fonctions privilégiées, notamment de désactiver, de contourner ou de modifier les mesures/contre-mesures de sécurité mises en œuvre.	iam-root-access-key-vérifier	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17(1)	Le système d'information surveille et contrôle les méthodes d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	s3- bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	alb-http-drop-invalid-activé par en-tête	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17(2)	Le système d'information met en œuvre des mécanismes de chiffrement pour protéger la confidentialité et l'intégrité des sessions d'accès à distance.	elb-tls-https-listeners-uniquement	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-17 (3)	Le système d'information achemine tous les accès distants via [Attribution : nombre défini par l'organisation] points de contrôle d'accès réseau gérés.	internet-gateway-authorized-vpc-uniquement	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées s qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21 (b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	ebs-snapshot-public-restorable-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	emr-master-no-public-IP	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	lambda-function-public-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	rds-instance-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AC-21(b)	L'organisation : b. Utilise [Attribution : mécanismes automatisés ou processus manuels définis par l'organisation] pour aider les utilisateurs à prendre des décisions en matière de partage d'informations/de collaboration.	sagemaker-notebook-no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2 (a) (d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	api-gw-execution-logging-activé	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du Compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2 (a) (d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de tous Régions AWS vers votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			sans avoir à faire quoi que ce soit.
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	s3- bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2 (a) (d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-2(a)(d)	L'organisation : a. Détermine que le système d'information est capable d'auditer les événements suivants : [Attribution : événements vérifiables définis par l'organisation] ; d. Détermine que les événements suivants doivent être vérifiés dans le système d'information : [Attribution : événements vérifiés définis par l'organisation (sous-ensemble des événements vérifiables définis dans AU-2 a.), ainsi que la fréquence d'un audit pour chaque événement identifié (ou la situation en nécessitant une)].	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	api-gw-execution-logging-activé	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du Compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de tous Régions AWS vers votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			sans avoir à faire quoi que ce soit.
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	s3- bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-3	Le système d'information génère des enregistrements d'audit contenant des informations qui établissent quel type d'événement s'est produit, quand l'événement s'est produit, où l'événement s'est produit, la source de l'événement, le résultat de l'événement et l'identité de toute personne ou sujet associé à l'événement.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanismes automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisationnels d'enquête et de réponse aux activités suspectes. (3) L'organisation analyse et met en corrélation les enregistrements d'audit de différents répertoires afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-6(1)(3)	(1) L'organisation utilise des mécanisme s automatisés pour intégrer les processus d'audit, d'analyse et de génération de rapports afin de faciliter les processus organisat ionnels d'enquête et de réponse aux activités suspectes . (3) L'organis ation analyse et met en corrélati on les enregistr ements d'audit de différents répertoir es afin d'obtenir une meilleure visibilité de la situation à l'échelle de l'organisation.	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-7(1)	Le système d'information permet de traiter les enregistrements d'audit pour les événements intéressants en fonction de [Attribution : champs d'audit définis par l'organisation dans les enregistrements d'audit].	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-7 (1)	Le système d'information permet de traiter les enregistrements d'audit pour les événements intéressants en fonction de [Attribution : champs d'audit définis par l'organisation dans les enregistrements d'audit].	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
AU-9	Le système d'information protège les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
AU-9	Le système d'information protège les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-9(2)	Le système d'information sauvegarde les enregistrements d'audit [Attribution : fréquence définie par l'organisation] sur un système ou un composant du système physiquement différent du système ou du composant vérifié.	s3- bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-11	L'organisation conserve les dossiers d'audit pendant [Affectation : période définie par l'organisation conformément à la politique de conservation des dossiers] afin de soutenir les after-the-fact enquêtes sur les incidents de sécurité et de répondre aux exigences réglementaires et organisationnelles en matière de conservation des informations.	cw-loggroup-retention-period-vérifier	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	api-gw-execution-logging-activé	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du Compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12 (a) (c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de tous Régions AWS vers votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			sans avoir à faire quoi que ce soit.
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	s3- bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12 (a) (c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
AU-12(a)(c)	Le système d'information : a. Permet de générer des enregistrements d'audit pour les événements vérifiables définis dans AU-2 a. à [Attribution : composants du système d'information définis par l'organisation] ; c. Génère des enregistrements d'audit pour les événements définis dans AU-2 d. avec le contenu défini dans AU-3.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveilla nce et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance.	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveilla nce et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance.	ec2- instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CA-7(a)(b)	L'organisation élabore une stratégie de surveillance continue et met en œuvre un programme de surveillance continue qui comprend : a. Établissement de [Attribution : métriques définies par l'organisation] à surveiller ; b. Établissement de [Attribution : fréquences définies par l'organisation] pour la surveillance et [Attribution : fréquences définies par l'organisation] pour les évaluations afin de faciliter cette surveillance.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2- -check managedinstance-association-compliance-status	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	ec2- volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-2	L'organisation élabore, documente et maintient, sous contrôle de configuration, une configuration de référence actuelle du système d'information.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-7(a)	L'organisation : a. Configure le système d'information pour qu'il ne fournisse que les fonctionnalités essentielles.	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-7(a)	L'organisation : a. Configure le système d'information pour qu'il ne fournisse que les fonctionnalités essentielles.	ec2- -check managedinstance-association-compliance-status	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-8(1)	L'organisation met à jour l'inventaire des composants du système d'informa tion en tant que partie intégrante des installations, des suppressions et des mises à jour du système d'informa tion.	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-8(3)(a)	L'organisation : a. Utilise des mécanismes automatisés [Attribution : fréquence définie par l'organisation] pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-8(3)(a)	L'organisation : a. Utilise des mécanismes automatisés [Attribution : fréquence définie par l'organisation] pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information	ec2- -check managedinstance-association-compliance-status	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CM-8(3)(a)	L'organisation : a. Utilise des mécanismes automatisés [Attribution : fréquence définie par l'organisation] pour détecter la présence de composants matériels, logiciels et micrologiciels non autorisés dans le système d'information	ec2- -check managedinstance-patch-compliance-status	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'informa tion [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'information [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'informa tion [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	elasticache-redis-cluster-automatic-vérification des sauvegardes	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'informa tion [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	s3- bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'information [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'information [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'informa tion [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-9(b)	L'organisation : b. Effectue des sauvegardes des informations de niveau système contenues dans le système d'information [Attribution : fréquence définie par l'organisation et compatible avec les objectifs en matière de délai et de point de récupération].	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	s3- bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	elasticache-redis-cluster-automatic-vérification des sauvegardes	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	s3- bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interruption, une compromission ou une panne.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	elb-cross-zone-load-activé pour l'équilib rage	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
CP-10	L'organisation assure la récupération et la reconstitution du système d'information dans un état connu après une interrupt ion, une compromis sion ou une panne.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-2	Le système d'information identifie et authentifie de manière unique les utilisateurs de l'organisation (ou les processus agissant pour le compte des utilisateurs de l'organisation).	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et le Centers for Internet Security (CIS) AWS Foundations Benchmark en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-2 (1) (11)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (11) Le système d'information met en œuvre une authentification multifactorielle pour l'accès à distance aux comptes privilégiés et non privilégiés, de telle sorte que l'un des facteurs soit fourni par un appareil distinct du système accédant et que l'appareil réponde à [Attribution : exigences du mécanisme définies par l'organisation].	root-account-hardware-mfa-activé	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-2 (1) (11)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (11) Le système d'information met en œuvre une authentification multifactorielle pour l'accès à distance aux comptes privilégiés et non privilégiés, de telle sorte que l'un des facteurs soit fourni par un appareil distinct du système accédant et que l'appareil réponde à [Attribution : exigences du mécanisme définies par l'organisation].	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-2 (1) (2) (11)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (2) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes non privilégiés. (11) Le système d'information met en œuvre une authentification multifactorielle pour l'accès à distance aux comptes privilégiés et non privilégiés, de telle sorte que l'un des facteurs soit fourni par un appareil distinct du système accédant et que l'appareil réponde à [Attribution : exigences du mécanisme définies par l'organisation].	mfa-enabled-for-iam-accès à la console	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-2 (1) (2) (11)	(1) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes privilégiés. (2) Le système d'information met en œuvre une authentification multifactorielle pour l'accès réseau aux comptes non privilégiés. (11) Le système d'information met en œuvre une authentification multifactorielle pour l'accès à distance aux comptes privilégiés et non privilégiés, de telle sorte que l'un des facteurs soit fourni par un appareil distinct du système accédant et que l'appareil réponde à [Attribution : exigences du mécanisme définies par l'organisation].	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-5 (1) (a) (d) (e)	Le système d'information, pour l'authentification par mot de passe : a. Applique une complexité minimale des mots de passe de [Attribution : exigences définies par l'organisation pour la sensibilité à la casse, le nombre de caractères, la combinaison de lettres majuscules, de lettres minuscules, de chiffres et de caractères spéciaux, y compris les exigences minimales pour chaque type] ; d. Applique des restrictions de durée de vie minimale et maximale des mots de passe de [Attribution : nombres définis par l'organisation pour la durée de vie minimale, la durée de vie maximale] ; e. Interdit la réutilisation des mots de passe pour [Attribution : nombre défini	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et le Centers for Internet Security (CIS) AWS Foundations Benchmark en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	par l'organisation] générations.		de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-5(4)	L'organisation utilise des outils automatisés pour déterminer si les authentificateurs de mots de passe sont suffisamment puissants pour satisfaire [Attribution : exigences définies par l'organisation].	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et le Centers for Internet Security (CIS) AWS Foundations Benchmark en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IA-5(7)	L'organisation veille à ce que les authentif icateurs statiques non chiffrés ne soient pas intégrés à des applications ou des scripts d'accès, ni stockés sur des touches de fonction.	codebuild-project-envvar-awscred-vérifier	Assurez-vous que les informations d'authent ification AWS_ACCES S_KEY_ID et AWS_SECRE T_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild . AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une expositio n involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IR-4(1)	L'organisation utilise des mécanismes automatisés pour faciliter le processus de gestion des incidents.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IR-4 (1)	L'organisation utilise des mécanismes automatisés pour faciliter le processus de gestion des incidents.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IR-6(1)	L'organisation utilise des mécanismes automatisés pour faciliter le signalement des incidents de sécurité.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
IR-7(1)	L'organisation utilise des mécanismes automatisés pour améliorer la disponibilité des informations et de la prise en charge liées à la réponse aux incidents.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
RA-5	L'organisation : a. Recherche les vulnérabilités dans le système d'information et les applications hébergées [Attribution : fréquence définie par l'organisation et/ou de manière aléatoire conformément au processus défini par l'organisation] et lorsque de nouvelles vulnérabilités susceptibles d'affecter le système/les applications sont identifiées et signalées ; b. Utilise des outils et des techniques d'analyse des vulnérabilités qui facilitent l'interopérabilité entre les outils et automatisent certaines parties du processus de gestion des vulnérabilités en utilisant des normes pour : 1. L'énumération des plateformes, des failles logicielles et des configurations	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	inappropriées ; 2. Le formatage des listes de contrôle et des procédures de test ; et 3. La mesure de l'impact des vulnérabilités ; c. Analyse les rapports d'analyse des vulnérabilités et les résultats des évaluations de contrôle de la sécurité ; d. Corrige les vulnérabilités légitimes [Attribution : temps de réponse définis par l'organisation], conformément à une évaluation organisationnelle des risques ; et e. Partage les informations obtenues dans le cadre du processus d'analyse des vulnérabilités et des évaluations de contrôle de la sécurité avec [Attribution : personnel ou rôles définis par l'organisation] pour faciliter l'élimination des vulnérabi		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	lités similaires dans d'autres systèmes d'information (c'est-à-dire les faiblesses ou déficiences systémiques).		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
RA-5	L'organisation : a. Recherche les vulnérabilités dans le système d'information et les applications hébergées [Attribution : fréquence définie par l'organisation et/ou de manière aléatoire conformément au processus défini par l'organisation] et lorsque de nouvelles vulnérabilités susceptibles d'affecter le système/les applications sont identifiées et signalées ; b. Utilise des outils et des techniques d'analyse des vulnérabilités qui facilitent l'interopérabilité entre les outils et automatisent certaines parties du processus de gestion des vulnérabilités en utilisant des normes pour : 1. L'énumération des plateformes, des failles logicielles et des configurations	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	inappropriées ; 2. Le formatage des listes de contrôle et des procédures de test ; et 3. La mesure de l'impact des vulnérabilités ; c. Analyse les rapports d'analyse des vulnérabilités et les résultats des évaluations de contrôle de la sécurité ; d. Corrige les vulnérabilités légitimes [Attribution : temps de réponse définis par l'organisation], conformément à une évaluation organisationnelle des risques ; et e. Partage les informations obtenues dans le cadre du processus d'analyse des vulnérabilités et des évaluations de contrôle de la sécurité avec [Attribution : personnel ou rôles définis par l'organisation] pour faciliter l'élimination des vulnérabi		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	lités similaires dans d'autres systèmes d'information (c'est-à-dire les faiblesses ou déficiences systémiques).		
SA-3(a)	L'organisation : a. Gère le système d'information en utilisant [Attribution : cycle de vie du développement du système défini par l'organisation] qui intègre des considérations relatives à la sécurité de l'information.	codebuild-project-envvar-awscred-vérifier	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SA-3(a)	L'organisation : a. Gère le système d'information en utilisant [Attribution : cycle de vie du développement du système défini par l'organisation] qui intègre des considérations relatives à la sécurité de l'information.	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SA-3(a)	L'organisation : a. Gère le système d'information en utilisant [Attribution : cycle de vie du développement du système défini par l'organisation] qui intègre des considérations relatives à la sécurité de l'information.	codebuild-project-source-repo-vérification de l'URL	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SA-10	L'organisation exige que le développeur du système d'information, du composant du système ou du service du système d'information : a. Effectue la gestion de la configuration au cours [Sélection (un ou plusieurs) : de la conception ; du développement ; de la mise en œuvre ; de l'exploitation] du système, du composant ou du service ; b. Documente, gère et contrôle l'intégrité des modifications apportées à [Attribution : éléments de configuration définis par l'organisation dans le cadre de la gestion de la configuration] ; c. Mette en œuvre uniquement les modifications approuvées par l'organisation	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	dans le système, le composant ou le service ; d. Documente les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SA-10	L'organisation exige que le développeur du système d'information, du composant du système ou du service du système d'information : a. Effectue la gestion de la configuration au cours [Sélection (un ou plusieurs) : de la conception ; du développement ; de la mise en œuvre ; de l'exploitation] du système, du composant ou du service ; b. Documente, gère et contrôle l'intégrité des modifications apportées à [Attribution : éléments de configuration définis par l'organisation dans le cadre de la gestion de la configuration] ; c. Mette en œuvre uniquement les modifications approuvées par l'organisation	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	dans le système, le composant ou le service ; d. Documente les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SA-10	L'organisation exige que le développeur du système d'informa tion, du composant du système ou du service du système d'information : a. Effectue la gestion de la configuration au cours [Sélectio n (un ou plusieurs) : de la conceptio n ; du développe ment ; de la mise en œuvre ; de l'exploit ation] du système, du composant ou du service ; b. Documente, gère et contrôle l'intégri té des modificat ions apportées à [Attribution : éléments de configura tion définis par l'organisation dans le cadre de la gestion de la configura tion] ; c. Mette en œuvre uniquemen t les modificat ions approuvées par l'organisation	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	dans le système, le composant ou le service ; d. Documente les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SA-10	L'organisation exige que le développeur du système d'information, du composant du système ou du service du système d'information : a. Effectue la gestion de la configuration au cours [Sélection (un ou plusieurs) : de la conception ; du développement ; de la mise en œuvre ; de l'exploitation] du système, du composant ou du service ; b. Documente, gère et contrôle l'intégrité des modifications apportées à [Attribution : éléments de configuration définis par l'organisation dans le cadre de la gestion de la configuration] ; c. Mette en œuvre uniquement les modifications approuvées par l'organisation	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	dans le système, le composant ou le service ; d. Documente les modifications approuvées apportées au système, au composant ou au service, ainsi que les impacts potentiel s de ces modificat ions sur la sécurité ; et e. Assure le suivi des failles de sécurité et leur résolution au sein du système, du composant ou du service et rende compte des résultats à [Attribution : personnel défini par l'organisation].		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-2	Le système d'information sépare les fonctionnalités utilisateur (y compris les services d'interface utilisateur) des fonctionnalités de gestion du système d'information.	iam-group-has-users-vérifier	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-2	Le système d'information sépare les fonctionnalités utilisateur (y compris les services d'interface utilisateur) des fonctionnalités de gestion du système d'information.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-4	Le système d'information empêche le déplacement d'informations non autorisé et involontaire via des ressources système partagées.	ec2- volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	autoscaling-group-elb-healthcheck-obligatoire	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	s3- bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	elb-cross-zone-load-activé pour l'équilibrage	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-5	Le système d'information se protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Attribution : types d'attaques par déni de service définis par l'organisation ou références aux sources de ces informations] en utilisant [Attribution : mesures de sécurité définies par l'organisation].	rds-instance-deletion-protection-activé	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3- bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	elb-tls-https-listeners-uniquement	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	ec2- instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	internet-gateway-authorized-vpc-uniquement	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	ebs-snapshot-public-restorable-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	emr-master-no-public-IP	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	lambda-function-public-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			Lambda doivent être attribuées à un VPC.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	rds-instance-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	sagemaker-notebook-no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	vpc-default-security-group-fermé	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	s3- bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	alb-http-drop-invalid-activé par en-tête	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7	Le système d'information : a. Surveille et contrôle les communications aux limites externes du système et aux limites internes clés du système ; b. Implémente des sous-réseaux pour les composants du système accessibles au public qui sont [Sélection : physiquement ; logiquement] séparés des réseaux organisationnels internes ; et c. Se connecte à des réseaux ou à des systèmes d'information externes uniquement par l'intermédiaire d'interfaces gérées constituées de dispositifs de protection des limites organisés conformément à une architecture de sécurité organisationnelle.	elasticsearch-node-to-node-vérification du chiffrement	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7 (3)	L'organisation limite le nombre de connexion s réseau externes au système d'informa tion.	ec2- instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	internet-gateway-authorized-vpc-uniquement	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7 (3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	ebs-snapshot-public-restorable-vérifier	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	ec2- instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	emr-master-no-public-IP	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	lambda-function-public-access-interdit	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	rds-instance-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	redshift-cluster-public-access-vérifier	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	blocs s3 account-level-public-access -	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	s3- bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	s3- bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	s3- bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	sagemaker-notebook-no-direct-accès à Internet	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	vpc-default-security-group-fermé	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-7(3)	L'organisation limite le nombre de connexions réseau externes au système d'information.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des informations transmises.	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des informations transmises.	alb-http-drop-invalid-activé par en-tête	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des informations transmises.	elasticsearch-node-to-node-vérification du chiffrement	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des informations transmises.	elb-tls-https-listeners-uniquement	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des informations transmises.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des informations transmises.	s3- bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des informations transmises.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	alb-http-drop-invalid-activé par en-tête	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8(1)	Le système d'informa tion met en œuvre des mécanisme s de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgati on non autorisée d'informations ; détecter les modificat ions apportées aux informations] pendant la transmiss ion, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	elasticsearch-node-to-node-vérification du chiffrement	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	elb-tls-https-listeners-uniquement	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	s3- bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-8(1)	Le système d'information met en œuvre des mécanismes de chiffrement pour [Sélection (un ou plusieurs) : empêcher la divulgation non autorisée d'informations ; détecter les modifications apportées aux informations] pendant la transmission, à moins qu'il ne soit protégé par [Attribution : autres mesures de protection physique définies par l'organisation].	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-12	L'organisation établit et gère les clés de chiffrement nécessaires au chiffrement employé dans le système d'information conformément à [Attribution : exigences définies par l'organisation pour la génération, la distribution, le stockage, l'accès et la destruction des clés].	cmk-backing-key-rotation-activé	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
SC-12	L'organisation établit et gère les clés de chiffrement nécessaires au chiffrement employé dans le système d'information conformément à [Attribution : exigences définies par l'organisation pour la génération, la distribution, le stockage, l'accès et la destruction des clés].	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-12	L'organisation établit et gère les clés de chiffrement nécessaires au chiffrement employé dans le système d'information conformément à [Attribution : exigences définies par l'organisation pour la génération, la distribution, le stockage, l'accès et la destruction des clés].	kms-cmk-not-scheduled-pour suppression	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	api-gw-cache-enabledet crypté	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	compatible avec bucket-server-side-encryption s3	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	s3- bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	sagemaker-endpoint-configuration-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	sagemaker-notebook-instance-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre [Attribution : utilisations du chiffrement définies par l'organisation et type de chiffrement requis pour chaque utilisation] conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux réglementations et aux normes applicables.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-13	Le système d'information met en œuvre un chiffrement validé par les FIPS ou approuvé par la NSA, conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements et aux normes applicables.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
SC-23	Le système d'information protège l'authenticité des sessions de communication.	alb-http-to-https-vérification de redirection	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-23	Le système d'information protège l'authenticité des sessions de communication.	alb-http-drop-invalid-activé par en-tête	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23	Le système d'information protège l'authenticité des sessions de communication.	elb-tls-https-listeners-uniquement	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	api-gw-cache-enabledet crypté	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	kms-cmk-not-scheduled-pour suppression	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	s3- bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	compatible avec bucket-server-side-encryption s3	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	sagemaker-endpoint-configuration-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	sagemaker-notebook-instance-kms-configuré par clé	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	ec2- ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SC-28	Le système d'information protège [Sélection (un ou plusieurs) : la confidentialité ; l'intégrité] des [Attribution : informations au repos définies par l'organisation].	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SC-36	L'organisation distribue [Attribution : traitement et stockage définis par l'organisation] sur plusieurs sites physiques.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SC-36	L'organisation distribue [Attribution : traitement et stockage définis par l'organisation] sur plusieurs sites physiques.	s3- bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-2 (2)	L'organisation utilise des mécanismes automatisés [Attribution : fréquence définie par l'organisation] pour déterminer l'état des composants du système d'information en ce qui concerne la correction des failles.	ec2- -check managedinstance-patch-compliance-status	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-2(2)	L'organisation utilise des mécanismes automatisés [Attribution : fréquence définie par l'organisation] pour déterminer l'état des composants du système d'information en ce qui concerne la correction des failles.	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-2(2)	L'organisation utilise des mécanismes automatisés [Attribution : fréquence définie par l'organisation] pour déterminer l'état des composants du système d'information en ce qui concerne la correction des failles.	ec2- -check managedinstance-association-compliance-status	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4 (1)	L'organisation connecte et configure des outils individuels de détection d'intrusi on dans un système de détection d'intrusi on à l'échelle du système d'informa tion.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(2)	L'organisation utilise des outils automatisés pour analyser les événements en temps quasi réel.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
SI-4(2)	L'organisation utilise des outils automatis és pour analyser les événements en temps quasi réel.	ec2- instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4 (4)	Le système d'information surveille le trafic de communications entrant et sortant [Attribution : fréquence définie par l'organisation] pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(4)	Le système d'information surveille le trafic de communications entrant et sortant [Attribution : fréquence définie par l'organisation] pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(4)	Le système d'information surveille le trafic de communications entrant et sortant [Attribution : fréquence définie par l'organisation] pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4 (4)	Le système d'information surveille le trafic de communications entrant et sortant [Attribution : fréquence définie par l'organisation] pour détecter des activités ou des circonstances inhabituelles ou non autorisées.	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(5)	Le système d'information alerte [Attribution : personnel ou rôles définis par l'organisation] lorsque les indications suivantes de compromission ou de compromission potentielle se produisent : [Attribution : indicateurs de compromission définis par l'organisation].	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(16)	L'organisation met en corrélation les informations issues des outils de surveillance utilisés dans l'ensemble du système d'informa tion.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	wafv2-logging-enab led	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	cloud-trail-cloud-watch-activé pour les journaux	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-4(a)(b)(c)	L'organisation : a. Surveille le système d'information pour détecter : 1. Attaques et indicateurs d'attaques potentiel les conformém ent à [Attribution : objectifs de surveilla nce définis par l'organisation] ; et 2. Connexions locales, réseau et distantes non autorisées ; b. Identifie l'utilisation non autorisée du système d'information en utilisant [Attribut ion : techniques et méthodes définies par l'organisation] ; c. Déploie des dispositifs de contrôle : i) à des endroits stratégiques du système d'informa tion pour recueilli r des informations essentielles déterminé es par l'organis ation ; et ii) à des endroits ponctuels du système pour suivre des types spécifiqu	ec2- instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
	es de transactions présentant un intérêt pour l'organisation.		
SI-7	L'organisation utilise des outils d'audit de l'intégrité pour détecter les modificat ions non autorisée s des [Attribution : logiciels, microprog rammes et informati ons définis par l'organisation].	cloud-trail-log-file-activé pour la validatio n	Utilisez la validatio n des fichiers AWS CloudTrail journaux pour vérifier l'intégri té des CloudTrail journaux. La validatio n du fichier journal permet de détermine r si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison . Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informati que, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-7(1)	Le système d'information effectue un contrôle d'intégrité des [Attribution : logiciels, microprogrammes et informations définis par l'organisation] [Sélection (un ou plusieurs) : au démarrage ; à [Attribution : états transitoires ou événements relatifs à la sécurité définis par l'organisation] ; [Attribution : fréquence définie par l'organisation]].	ec2- -manager instance-managed-by-systems	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-7(1)	Le système d'information effectue un contrôle d'intégrité des [Attribution : logiciels, microprogrammes et informations définis par l'organisation] [Sélection (un ou plusieurs) : au démarrage ; à [Attribution : états transitoires ou événements relatifs à la sécurité définis par l'organisation] ; [Attribution : fréquence définie par l'organisation]].	ec2- -check managedinstance-patch-compliance-status	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-7(1)	Le système d'information effectue un contrôle d'intégrité des [Attribution : logiciels, microprogrammes et informations définis par l'organisation] [Sélection (un ou plusieurs) : au démarrage ; à [Attribution : états transitoires ou événements relatifs à la sécurité définis par l'organisation] ; [Attribution : fréquence définie par l'organisation]].	cloud-trail-log-file-activé pour la validation	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	s3- bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	elasticache-redis-cluster-automatic-vérification des sauvegardes	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Config Règle	Conseils
SI-12	L'organisation traite et conserve les informations contenues dans le système d'information et les informations produites par le système conformément aux lois fédérales, aux décrets, aux directives, aux politiques, aux règlements, aux normes et aux exigences opérationnelles applicables.	cw-loggroup-retention-period-vérifier	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST 800-53 rev 4.

Bonnes pratiques de fonctionnement pour NIST 800-53 rev 5

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le NIST 800-53 et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NIST 800-53. Un contrôle NIST 800-53 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (1)	Gestion de compte | Gestion automatisée des comptes système	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (3)	Gestion de compte | Désactiver les comptes	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (3)	Gestion de compte | Désactiver les comptes	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (3)	Gestion de compte | Désactiver les comptes	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (4)	Gestion de compte | Actions de vérification automatisées	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2 (12)	Gestion de compte | Surveillance des comptes en cas d'utilisation atypique	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	Gestion de compte	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	Gestion de compte	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	Gestion de compte	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	Gestion de compte	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-2	Gestion de compte	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	Gestion de compte	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-2	Gestion de compte	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (7)	Exécution d'accès | Contrôle d'accès basé sur les rôles	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3 (15)	Exécution d'accès | Contrôle d'accès discrétionnaire et obligatoire	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
AC-3	Exécution d'accès	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
AC-3	Exécution d'accès	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
AC-3	Exécution d'accès	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-3	Exécution d'accès	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-3	Exécution d'accès	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-3	Exécution d'accès	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-3	Exécution d'accès	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-3	Exécution d'accès	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes . Ces attaques Web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (21)	Exécution des flux d'informations | Séparation physique ou logique des flux d'informations	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4 (26)	Exécution des flux d'informations | Actions de filtrage des audits	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-4	Exécution du flux d'informations	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-4	Exécution du flux d'informations	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
AC-4	Exécution du flux d'informations	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
AC-4	Exécution du flux d'informations	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
AC-4	Exécution du flux d'informations	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-4	Exécution du flux d'informations	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AC-4	Exécution du flux d'informations	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-4	Exécution du flux d'informations	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
AC-4	Exécution du flux d'informations	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-4	Exécution du flux d'informations	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-4	Exécution du flux d'informations	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-4	Exécution du flux d'informations	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5	Séparation des tâches	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5	Séparation des tâches	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
AC-5	Séparation des tâches	iam-policy-no-stat ements-with-full-a ccess	Assurez-vous que les actions IAM sont limitées aux seules actions nécessair es. Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5	Séparation des tâches	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-5	Séparation des tâches	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-5	Séparation des tâches	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (2)	Moindre privilège | Accès non privilégié pour les fonctions non liées à la sécurité	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (2)	Moindre privilège | Accès non privilégié pour les fonctions non liées à la sécurité	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (2)	Moindre privilège | Accès non privilégié pour les fonctions non liées à la sécurité	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (3)	Moindre privilège | Accès réseau aux commandes privilégi ées	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (3)	Moindre privilège | Accès réseau aux commandes privilégiées	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (3)	Moindre privilège | Accès réseau aux commandes privilégi ées	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (3)	Moindre privilège | Accès réseau aux commandes privilégi ées	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-6 (3)	Moindre privilège | Accès réseau aux commandes privilégiées	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (3)	Moindre privilège | Accès réseau aux commandes privilégiées	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (9)	Moindre privilège | Consigner l'utilisation des fonctions privilégiées	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (10)	Moindre privilège | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (10)	Moindre privilège | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6 (10)	Moindre privilège | Interdire aux utilisateurs non privilégiés d'exécuter des fonctions privilégiées	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
AC-6	Principe de moindre privilège	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-6	Principe de moindre privilège	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
AC-6	Principe de moindre privilège	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-6	Principe de moindre privilège	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
AC-6	Principe de moindre privilège	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-6	Principe de moindre privilège	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-6	Principe de moindre privilège	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-6	Principe de moindre privilège	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 (2)	Accès à distance | Protection de la confidentialité et de l'intégrité à l'aide du chiffrement	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
AC-17 (2)	Accès à distance | Protection de la confidentialité et de l'intégrité à l'aide du chiffrement	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 (2)	Accès à distance | Protection de la confidentialité et de l'intégrité à l'aide du chiffrement	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
AC-17 (2)	Accès à distance | Protection de la confidentialité et de l'intégrité à l'aide du chiffrement	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 (2)	Accès à distance | Protection de la confidentialité et de l'intégrité à l'aide du chiffrement	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
AC-17 (2)	Accès à distance | Protection de la confidentialité et de l'intégrité à l'aide du chiffrement	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-17 (2)	Accès à distance | Protection de la confidentialité et de l'intégrité à l'aide du chiffrement	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
AC-21	Partage d'informations	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
AC-21	Partage d'informations	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
AC-21	Partage d'informations	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-21	Partage d'informations	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
AC-21	Partage d'informations	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
AC-21	Partage d'informations	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
AC-21	Partage d'informations	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AC-21	Partage d'informations	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-2	Journalisation des événements	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-2	Journalisation des événements	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-2	Journalisation des événements	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-3	Contenu des enregistrements d'audit	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-3	Contenu des enregistrements d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-3	Contenu des enregistrements d'audit	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
AU-6 (1)	Examen, analyse et rapports des enregistrements d'audit | Intégration automatisée des processus	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (1)	Examen, analyse et rapports des enregistrements d'audit | Intégration automatisée des processus	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (1)	Examen, analyse et rapports des enregistrements d'audit | Intégration automatisée des processus	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (1)	Examen, analyse et rapports des enregistrements d'audit | Intégration automatisée des processus	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (3)	Examen, analyse et rapports des enregistrements d'audit | Corréler les référentiels des enregistrements d'audit	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (4)	Examen, analyse et rapports des enregistrements d'audit | Examen et analyse centralisés	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
AU-6 (5)	Examen, analyse et rapports des enregistrements d'audit | Analyse intégrée des enregistrements d'audit	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (5)	Examen, analyse et rapports des enregistrements d'audit | Analyse intégrée des enregistrements d'audit	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (5)	Examen, analyse et rapports des enregistrements d'audit | Analyse intégrée des enregistrements d'audit	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-6 (5)	Examen, analyse et rapports des enregistrements d'audit | Analyse intégrée des enregistrements d'audit	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-7 (1)	Réduction des enregistrements d'audit et génération de rapports | Traitement automatique	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
AU-9 (2)	Protection des informations d'audit | Stockage sur des systèmes ou composants physiques distincts	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9 (2)	Protection des informations d'audit | Stockage sur des systèmes ou composants physiques distincts	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9 (2)	Protection des informations d'audit | Stockage sur des systèmes ou composants physiques distincts	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9 (7)	Protection des informations d'audit | Stockage sur un composant avec un système d'exploitation différent	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
AU-9	Protection des informations d'audit	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	Protection des informations d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.
AU-9	Protection des informations d'audit	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	Protection des informations d'audit	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-9	Protection des informations d'audit	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
AU-10	Non-répudiation	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-10	Non-répudiation	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
AU-10	Non-répudiation	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-10	Non-répudiation	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
AU-12	Génération d'enregis trements d'audit	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregistrements d'audit	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
AU-12	Génération d'enregis trements d'audit	cloud-trail-cloud- watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregistrements d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-12	Génération d'enregis trements d'audit	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
AU-14 (1)	Audit de session | Démarrage du système	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
CA-7	Surveillance continue	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
CA-7	Surveillance continue	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CA-7	Surveillance continue	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-7	Surveillance continue	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
CA-9 (1)	Connexions au système interne | Contrôles de conformité	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
CA-9 (1)	Connexions au système interne | Contrôles de conformité	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
CA-9 (1)	Connexions au système interne | Contrôles de conformité	rds-instance-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut contribuer à réduire la surface d'attaque de votre ou de vos instances de base de données Amazon Relational Database Service (Amazon RDS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
CA-9 (1)	Connexions au système interne | Contrôles de conformité	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
CA-9 (1)	Connexions au système interne | Contrôles de conformité	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.
CA-9 (1)	Connexions au système interne | Contrôles de conformité	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
CA-9 (1)	Connexions au système interne | Contrôles de conformité	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
CA-9 (1)	Connexions au système interne | Contrôles de conformité	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	redshift-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut réduire la surface d'attaque de votre ou de vos clusters Amazon Redshift.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
CA-9 (1)	Connexions au système interne | Contrôles de conformité	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CA-9 (1)	Connexions au système interne | Contrôles de conformité	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2 (2)	Configuration de base | Soutien à l'automatisation pour l'exactitude et l'actualité	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2 (2)	Configuration de base | Soutien à l'automatisation pour l'exactitude et l'actualité	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2 (2)	Configuration de base | Soutien à l'automatisation pour l'exactitude et l'actualité	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2 (2)	Configuration de base | Soutien à l'automatisation pour l'exactitude et l'actualité	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2 (2)	Configuration de base | Soutien à l'automatisation pour l'exactitude et l'actualité	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2 (2)	Configuration de base | Soutien à l'automatisation pour l'exactitude et l'actualité	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
CM-2	Configuration de référence	rds-instance-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut contribuer à réduire la surface d'attaque de votre ou de vos instances de base de données Amazon Relational Database Service (Amazon RDS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	redshift-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut réduire la surface d'attaque de votre ou de vos clusters Amazon Redshift.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-2	Configuration de référence	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3 (6)	Contrôle des modifications de configuration | Gestion du chiffrement	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
CM-3	Contrôle des modifications de configuration	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-3	Contrôle des modifications de configuration	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-7	Principe de moindre fonctionnalité	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-7	Principe de moindre fonctionnalité	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-7	Principe de moindre fonctionnalité	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8 (1)	Inventaire des composants système | Mises à jour lors de l'installation et de la suppression	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8 (1)	Inventaire des composants système | Mises à jour lors de l'installation et de la suppression	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8 (2)	Inventaire des composants système | Maintenance automatisée	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8 (3)	Inventaire des composants système | Détection automatisée des composants non autorisés	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8 (3)	Inventaire des composants système | Détection automatisée des composants non autorisés	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8 (3)	Inventaire des composants système | Détection automatisée des composants non autorisés	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8 (3)	Inventaire des composants système | Détection automatisée des composants non autorisés	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8	Inventaire des composants système	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CM-8	Inventaire des composants système	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-2 (2)	Plan d'urgence | Planification des capacités	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-2 (2)	Plan d'urgence | Planification des capacités	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (1)	Site de stockage alternatif | Séparation du site principal	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6 (2)	Site de stockage alternatif | Objectifs en matière de délai et de point de récupération	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-6	Site de stockage alternatif	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-9	Sauvegarde du système	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
CP-10	Reprise et reconstitution du système	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CP-10	Reprise et reconstitution du système	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (1)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes privilégi és	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (1)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes privilégi és	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (1)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes privilégiés	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (1)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes privilégiés	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (2)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes non privilégiés	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (2)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes non privilégiés	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (2)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes non privilégiés	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (2)	Identification et authentification (utilisateurs de l'organisation) | Authentification multifactorielle pour les comptes non privilégiés	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (6)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — appareil distinct	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (6)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — appareil distinct	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (6)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — appareil distinct	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (6)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — appareil distinct	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (8)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — résistant aux réexécutions	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (8)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — résistant aux réexécutions	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (8)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — résistant aux réexécutions	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-2 (8)	Identification et authentification (utilisateurs de l'organisation) | Accès aux comptes — résistant aux réexécutions	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 (1)	Gestion des authentif icateurs | Authentif ication par mot de passe	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IA-5 (7)	Gestion des authentificateurs | Aucun authentificateur statique non chiffré intégré	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4 (1)	Gestion des incidents | Processus automatisés de gestion des incidents	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
IR-4 (5)	Gestion des incidents | Désactivation automatique du système	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RA-3 (4)	Évaluation des risques | Cyberanalyse prédictive	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-3	Cycle de vie du développement du système	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-3	Cycle de vie du développement du système	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-8 (19)	Principes d'ingénierie en matière de sécurité et de confidentialité | Protection continue	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-8 (21)	Principes d'ingénierie en matière de sécurité et de confidentialité | Auto-analyse	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-8 (22)	Principes d'ingénierie en matière de sécurité et de confidentialité | Responsabilité et traçabilité	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-8 (25)	Principes d'ingénierie en matière de sécurité et de confidentialité | Sécurité économique	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-11 (1)	Tests et évaluations pour les développe urs | Analyse de code statique	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-11 (6)	Tests et évaluations pour les développe urs | Évaluations de la surface d'attaque	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-15 (2)	Processus, normes et outils de développement | Outils de suivi de la sécurité et de la confidentialité	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-15 (2)	Processus, normes et outils de développement | Outils de suivi de la sécurité et de la confidentialité	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-15 (8)	Processus, normes et outils de développement | Réutilisation des informations sur les menaces et les vulnérabilités	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SA-15 (8)	Processus, normes et outils de développement | Réutilisation des informations sur les menaces et les vulnérabilités	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (1)	enial-of-service Protection D | Limiter la capacité d'attaquer d'autres systèmes	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferred MaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (2)	D enial-of-service Protection | Capacité, bande passante et redondance	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5 (3)	D enial-of-service Protection | Détection et surveillance	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-5	enial-of-service Protection D	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7 (3)	Protection des limites | Points d'accès	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7 (3)	Protection des limites | Points d'accès	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (3)	Protection des limites | Points d'accès	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (3)	Protection des limites | Points d'accès	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7 (3)	Protection des limites | Points d'accès	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7 (3)	Protection des limites | Points d'accès	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (3)	Protection des limites | Points d'accès	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-7 (4)	Protection des limites | Services de télécommunications externes	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7 (4)	Protection des limites | Services de télécommunications externes	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
SC-7 (4)	Protection des limites | Services de télécommunications externes	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7 (4)	Protection des limites | Services de télécommunications externes	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
SC-7 (4)	Protection des limites | Services de télécommunications externes	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (4)	Protection des limites | Services de télécommunications externes	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-7 (4)	Protection des limites | Services de télécommunications externes	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7 (4)	Protection des limites | Services de télécommunications externes	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
SC-7 (4)	Protection des limites | Services de télécommunications externes	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7 (4)	Protection des limites | Services de télécommunications externes	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-7 (4)	Protection des limites | Services de télécommunications externes	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (4)	Protection des limites | Services de télécommunications externes	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (5)	Protection des limites | Rejeter par défaut — Autoriser par exception	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (5)	Protection des limites | Rejeter par défaut — Autoriser par exception	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (5)	Protection des limites | Rejeter par défaut — Autoriser par exception	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (5)	Protection des limites | Rejeter par défaut — Autoriser par exception	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (9)	Protection des limites | Limiter le trafic des communications sortantes menaçantes	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
SC-7 (10)	Protection des limites | Empêcher l'exfiltr ation	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (10)	Protection des limites | Empêcher l'exfiltration	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (11)	Protection des limites | Limiter le trafic des communications entrantes	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (16)	Protection des limites | Empêcher la découverte de composants système	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (20)	Protection des limites | Isolation et séparation dynamiques	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7 (21)	Protection des limites | Isolation des composants système	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7 (21)	Protection des limites | Isolation des composants système	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (21)	Protection des limites | Isolation des composants système	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7 (21)	Protection des limites | Isolation des composants système	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7 (21)	Protection des limites | Isolation des composants système	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7 (21)	Protection des limites | Isolation des composants système	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7 (21)	Protection des limites | Isolation des composants système	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
SC-7	Protection des limites	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
SC-7	Protection des limites	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7	Protection des limites	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
SC-7	Protection des limites	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
SC-7	Protection des limites	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
SC-7	Protection des limites	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-7	Protection des limites	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (1)	Confidentialité et intégrité des transmissions | Protection par le chiffrement	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8 (2)	Confidentialité et intégrité des transmissions | Gestion avant et après transmission	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Confidentialité et intégrité des transmissions	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Confidentialité et intégrité des transmissions	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-8	Confidentialité et intégrité des transmissions	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Confidentialité et intégrité des transmissions	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
SC-8	Confidentialité et intégrité des transmissions	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Confidentialité et intégrité des transmissions	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-8	Confidentialité et intégrité des transmissions	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Confidentialité et intégrité des transmissions	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-8	Confidentialité et intégrité des transmissions	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-8	Confidentialité et intégrité des transmissions	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés symétriques	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés symétriques	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés asymétriques	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés asymétriques	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés asymétriques	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés asymétriques	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés asymétriques	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés asymétriques	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12 (2)	Établissement et gestion des clés de chiffrement | Clés asymétriques	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-12	Établissement et gestion des clés de chiffrement	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-12	Établissement et gestion des clés de chiffrement	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
SC-13	Protection par le chiffrement	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
SC-13	Protection par le chiffrement	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-13	Protection par le chiffrement	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
SC-13	Protection par le chiffrement	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-13	Protection par le chiffrement	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC-13	Protection par le chiffrement	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
SC-13	Protection par le chiffrement	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
SC-13	Protection par le chiffrement	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SC-13	Protection par le chiffrement	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC-13	Protection par le chiffrement	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-13	Protection par le chiffrement	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
SC-13	Protection par le chiffrement	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SC-13	Protection par le chiffrement	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
SC-13	Protection par le chiffrement	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-13	Protection par le chiffrement	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 (3)	Authenticité des sessions | Identifiants de session uniques générés par le système	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 (5)	Authenticité des sessions | Autorités de certification autorisées	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23 (5)	Authenticité des sessions | Autorités de certification autorisées	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Authenticité des sessions	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23	Authenticité des sessions	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Authenticité des sessions	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
SC-23	Authenticité des sessions	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Authenticité des sessions	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-23	Authenticité des sessions	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Authenticité des sessions	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Authenticité des sessions	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SC-23	Authenticité des sessions	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-23	Authenticité des sessions	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (1)	Protection des informations au repos | Protection par le chiffrement	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28 (3)	Protection des informations au repos | Clés de chiffrement	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
SC-28 (3)	Protection des informations au repos | Clés de chiffrement	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.
SC-28	Protection des informations au repos	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
SC-28	Protection des informations au repos	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
SC-28	Protection des informations au repos	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
SC-28	Protection des informations au repos	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
SC-28	Protection des informations au repos	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SC-28	Protection des informations au repos	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
SC-28	Protection des informations au repos	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
SC-28	Protection des informations au repos	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SC-28	Protection des informations au repos	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-28	Protection des informations au repos	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-36 (2)	Traitement et stockage distribués | Synchronisation	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-36	Traitement et stockage distribués	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-36	Traitement et stockage distribués	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-36	Traitement et stockage distribués	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SC-36	Traitement et stockage distribués	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (2)	Correction des failles | État de la correction automatique des failles	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (2)	Correction des failles | État de la correctio n automatique des failles	elastic-beanstalk-managed-updates-en abled	L'activation des mises à jour de plateforme gérées pour un environne ment Amazon Elastic Beanstalk garantit l'installation des derniers correctif s, mises à jour et fonctionnalités de la plateforme disponibl es pour l'environ nement. La sécurisat ion des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (2)	Correction des failles | État de la correction automatique des failles	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (3)	Correction des failles | Délai pour remédier aux failles et critères de référence pour les mesures correctives	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (3)	Correction des failles | Délai pour remédier aux failles et critères de référence pour les mesures correctives	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (3)	Correction des failles | Délai pour remédier aux failles et critères de référence pour les mesures correctives	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (4)	Correction des failles | Outils de gestion automatique des correctifs	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (4)	Correction des failles | Outils de gestion automatique des correctifs	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (4)	Correction des failles | Outils de gestion automatique des correctifs	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (5)	Correction des failles | Mises à jour automatiques des logiciels et des microprogrammes	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (5)	Correction des failles | Mises à jour automatiques des logiciels et des microprogrammes	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2 (5)	Correction des failles | Mises à jour automatiques des logiciels et des microprogrammes	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
SI-2	Correction des failles	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-2	Correction des failles	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-3 (8)	Protection contre les codes malveillants | Détecter les commandes non autorisées	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (1)	Surveillance du système | Système de détection des intrusions à l'échelle du système	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (2)	Surveillance du système | Outils et mécanismes automatisés pour l'analyse en temps réel	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (4)	Surveillance du système | Trafic des communications entrantes et sortantes	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (4)	Surveillance du système | Trafic des communications entrantes et sortantes	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (5)	Surveillance du système | Alertes générées par le système	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (5)	Surveillance du système | Alertes générées par le système	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (5)	Surveillance du système | Alertes générées par le système	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (12)	Surveillance du système | Alertes automatisées générées par l'organisation	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (13)	Surveillance du système | Analyser les tendances en matière de trafic et d'événements	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (20)	Surveillance du système | Utilisateurs privilégiés	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (22)	Surveillance du système | Services réseau non autorisés	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4 (25)	Surveillance du système | Optimiser l'analyse du trafic réseau	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	Surveillance du système	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	Surveillance du système	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-4	Surveillance du système	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (1)	Intégrité des logiciels, des microprogrammes et des informations | Contrôles d'intégrité	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (3)	Intégrité des logiciels, des microprogrammes et des informations | Outils de gestion centralisée de l'intégrité	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (6)	Intégrité des logiciels, des microprogrammes et des informations | Protection par le chiffrement	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (7)	Intégrité des logiciels, des microprogrammes et des informations | Intégration de la détection et de la réponse	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-7 (8)	Intégrité des logiciels, des microprogrammes et des informations | Capacité d'audit pour les événements importants	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	Gestion et conservation des informations	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	Gestion et conservation des informations	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	Gestion et conservation des informations	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	Gestion et conservation des informations	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	Gestion et conservation des informations	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	Gestion et conservation des informations	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-12	Gestion et conservation des informations	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	s3-version-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-13 (5)	Prévention prévisible des défaillances | Capacité de basculement	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle réseau privé virtuel en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-20	Rejet	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-20	Rejet	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
SI-20	Rejet	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST 800-53 rev 5.

Bonnes pratiques de fonctionnement pour NIST 800 171

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le NIST 800-171 et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NIST 800-171. Un contrôle NIST 800-171 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés et aux appareils (y compris les autres systèmes).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés et aux appareils (y compris les autres systèmes).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés et aux appareils (y compris les autres systèmes).	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearc h Service. Le contrôle d'accès précis fournit des mécanisme s d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authent ification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisate urs autorisés, aux processus agissant au nom des utilisate urs autorisés et aux appareils (y compris les autres systèmes).	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.1	Limitez l'accès au système aux utilisateurs autorisés, aux processus agissant au nom des utilisateurs autorisés et aux appareils (y compris les autres systèmes).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.2	Limitez l'accès au système aux types de transactions et de fonctions que les utilisateurs autorisés ont le droit d'exécuter.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3	Contrôlez le flux de CUI conformément aux autorisations approuvées.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.4	Séparez les tâches des individus afin de réduire le risque d'activités malveillantes sans collusion.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
3.1.5	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.1.5	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège, y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.5	Utilisez le principe du moindre privilège , y compris pour des fonctions de sécurité spécifiques et des comptes privilégiés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.6	Utilisez des comptes ou des rôles non privilégiés pour accéder à des fonctions non liées à la sécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et vérifiez l'exécution de ces fonctions.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.7	Empêchez les utilisate urs non privilégi és d'exécuter des fonctions privilégiées et vérifiez l'exécution de ces fonctions.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et vérifiez l'exécution de ces fonctions.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et vérifiez l'exécution de ces fonctions.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et vérifiez l'exécution de ces fonctions.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et vérifiez l'exécution de ces fonctions.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.7	Empêchez les utilisateurs non privilégiés d'exécuter des fonctions privilégiées et vérifiez l'exécution de ces fonctions.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.12	Surveillez et contrôlez les sessions d'accès à distance.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	opensearch-https-r equired	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,113	Utilisez des mécanismes de chiffrement pour protéger la confident ialité des sessions d'accès à distance.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,114	Acheminez l'accès à distance via des points de contrôle d'accès gérés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,1,20	Vérifiez et contrôlez/limitez les connexions aux systèmes externes et leur utilisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.1	Créez et conservez des enregistrements d'audit du système dans la mesure nécessaire pour permettre la surveillance, l'analyse, l'investigation et le signalement d'activités illégales, non autorisées ou inappropriées du système.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.2	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.2	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.2	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.2	Assurez-vous que les actions des différents utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.2	Assurez-vous que les actions des différent s utilisateurs du système peuvent être retracées de manière unique jusqu'à ces utilisateurs afin qu'ils puissent être tenus pour responsables de leurs actions.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.4	Alerte en cas d'échec du processus d'audit.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.4	Alerte en cas d'échec du processus d'audit.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.5	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'audit à des fins d'enquête et de réponse aux indications d'activités inappropriées, suspectes ou inhabituelles.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.5	Mettez en corrélation les processus d'examen, d'analyse et de génération de rapports d'audit à des fins d'enquête et de réponse aux indications d'activités inappropriées, suspectes ou inhabituelles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3.8	Protégez les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-security-group -attached-to-eni-p eriodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveille r les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environne ment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.1	Élaborez et maintenez des configurations de référence et des inventaires de systèmes organisat ionnels (y compris du matériel, des logiciels, des microprogrammes et de la documenta tion) tout au long des cycles de développe ment des systèmes respectifs.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.
3.4.6	Utilisez le principe de moindre fonctionn alité en configura nt les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.4.6	Utilisez le principe de moindre fonctionnalité en configurant les systèmes de l'organisation de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.7	Limitez, désactivez et empêchez l'utilisation de fonctions, de ports, de protocoles ou de services non essentiel s.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.7	Limitez, désactivez et empêchez l'utilisation de fonctions, de ports, de protocoles ou de services non essentiel s.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.7	Limitez, désactivez et empêchez l'utilisation de fonctions, de ports, de protocoles ou de services non essentiel s.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.7	Limitez, désactivez et empêchez l'utilisation de fonctions, de ports, de protocoles ou de services non essentiel s.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.9	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.9	Contrôlez et surveillez les logiciels installés par l'utilisateur.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes de l'organisation.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes de l'organisation.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2	Authentifiez (ou vérifiez) l'identité de ces utilisateurs, processus ou appareils, comme condition préalable pour autoriser l'accès aux systèmes de l'organisation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.3	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.3	Utilisez l'authent ification multifact orielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.3	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.3	Utilisez l'authentification multifactorielle pour l'accès local et réseau aux comptes privilégiés et pour l'accès réseau aux comptes non privilégiés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.5	Empêchez la réutilisation des identifiants pendant une période définie.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.6	Désactivez les identifiants au bout d'une période d'inactivité définie.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.7	Exigez une complexité minimale des mots de passe et un changement de caractères lors de la création de nouveaux mots de passe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.8	Interdisez la réutilisation des mots de passe pendant un certain nombre de générations.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.10	Stockez et transmettez uniquement des mots de passe protégés par chiffrement.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-non-arch ived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuell ement daysLowSe v (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	cloudwatch-alarm-a ction-check	Amazon CloudWatc h émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActi onRequired (Config Default : True), insufficientDataAc tion Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.1	Établissez une capacité opération nelle de traitement des incidents pour les systèmes de l'organis ation, qui comprend des activités de préparation, de détection, d'analyse , de confinement, de récupération et de réponse des utilisate urs.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.11.2	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant le système sont identifiées.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.11.2	Recherchez régulièrement les vulnérabilités dans les systèmes et applications de l'organisation et lorsque de nouvelles vulnérabilités affectant le système sont identifiées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.11.3	Corrigez les vulnérabilités conformément aux évaluations des risques.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.1	Surveillez, contrôlez et protégez les communications (c'est-à-dire les informations transmises ou reçues par les systèmes de l'organisation) aux limites externes et aux principales limites internes des systèmes de l'organisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	ec2-instance-no-pu blic-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearch Service. Le contrôle d'accès précis fournit des mécanismes d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authentification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptio ns architecturales, des techniques de développement de logiciels et des principes d'ingénie rie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.2	Utilisez des conceptions architecturales, des techniques de développement de logiciels et des principes d'ingénierie des systèmes qui favorisent une sécurité efficace de l'information au sein des systèmes de l'organisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13,6	Refusez le trafic de communications réseau par défaut et autorisez le trafic de communications réseau par exception (c'est-à-dire, tout refuser, autoriser par exception).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13,6	Refusez le trafic de communications réseau par défaut et autorisez le trafic de communications réseau par exception (c'est-à-dire, tout refuser, autoriser par exception).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13,6	Refusez le trafic de communications réseau par défaut et autorisez le trafic de communications réseau par exception (c'est-à-dire, tout refuser, autoriser par exception).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,8	Mettez en œuvre des mécanismes de chiffrement pour empêcher la divulgation non autorisée de CUI pendant la transmission, sous réserve de l'application d'autres mesures de protection physique.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3,13,10	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,10	Établissez et gérez des clés de chiffrement pour le chiffrement utilisé dans les systèmes de l'organisation.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confidentialité des CUI au repos.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
3,13,16	Protégez la confidentialité des CUI au repos.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confidentialité des CUI au repos.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
3,13,16	Protégez la confidentialité des CUI au repos.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confidentialité des CUI au repos.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confident ialité des CUI au repos.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confidentialité des CUI au repos.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
3,13,16	Protégez la confidentialité des CUI au repos.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
3,13,16	Protégez la confidentialité des CUI au repos.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confident ialité des CUI au repos.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
3,13,16	Protégez la confident ialité des CUI au repos.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
3,13,16	Protégez la confident ialité des CUI au repos.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confidentialité des CUI au repos.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
3,13,16	Protégez la confidentialité des CUI au repos.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confident ialité des CUI au repos.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confidentialité des CUI au repos.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,13,16	Protégez la confident ialité des CUI au repos.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
3,13,16	Protégez la confident ialité des CUI au repos.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.1	Identifiez, signalez et corrigez les informati ons et les failles du système en temps voulu.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.1	Identifiez, signalez et corrigez les informations et les failles du système en temps voulu.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2	Assurez la protection contre les codes malveillants aux endroits appropriés dans les systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.3	Surveillez les alertes et les avis de sécurité du système et prenez les mesures qui s'imposent.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.4	Mettez à jour les mécanismes de protection contre les codes malveillants lorsque de nouvelles versions sont disponibles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiellles.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiellles.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiellement.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,6	Surveillez les systèmes de l'organisation, y compris le trafic des communications entrantes et sortantes, afin de détecter les attaques et les indicateurs d'attaques potentiels.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14,7	Identifiez les utilisations non autorisées des systèmes de l'organisation.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST 800 171.

Bonnes pratiques de fonctionnement pour NIST 800 172

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le NIST 800-172 et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et

concerne un ou plusieurs contrôles NIST 800-172. Un contrôle NIST 800-172 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	clb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	ec2-token-hop-limit-check	Assurez-vous que la réponse HTTP PUT du service de métadonnées d'instance (IMDS) est limitée à l'instance Amazon Elastic Compute Cloud (Amazon EC2). Avec IMDSv2, la réponse PUT qui contient le jeton secret ne peut pas, par défaut, sortir de l'instance, car la limite des tronçons de la réponse Metadata est fixée à 1 (configuration par défaut). Si cette valeur est supérieure à 1, le jeton peut quitter l'instance EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1.3e	Utilisez [Attribution : solutions de transfert d'informations sécurisées définies par l'organisation] pour contrôler les flux d'informations entre les domaines de sécurité sur les systèmes connectés.	nacl-no-unrestricted-ssh-rdp	L'accès aux ports d'administration des serveurs distants figurant dans vos listes de contrôle d'accès au réseau (NACL), tels que le port 22 (SSH) et le port 3389 (RDP), ne doit pas être accessible au public, car cela pourrait permettre un accès imprévu à des ressources au sein de votre VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.2.1e	Dispensez une formation de sensibilisation [Attribution : fréquence définie par l'organisation] axée sur la reconnaissance et la réponse aux menaces liées à l'ingénierie sociale, aux acteurs de menaces persistantes avancées, aux brèches et aux comportements suspects ; mettez à jour la formation [Attribution : fréquence définie par l'organisation] ou lorsque des modifications importantes affectent la menace.	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.2e	Utilisez des mécanismes automatisés pour détecter les composants système mal configurés ou non autorisés ; après détection , [Sélection (un ou plusieurs) : retirez les composants; placez les composants dans un réseau de quarantaine ou de mise à jour] afin de faciliter l'application de correctifs, la reconfiguration ou d'autres mesures d'atténuation.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.2e	Utilisez des mécanismes automatisés pour détecter les composants système mal configurés ou non autorisés ; après détection , [Sélection (un ou plusieurs) : retirez les composants; placez les composants dans un réseau de quarantaine ou de mise à jour] afin de faciliter l'application de correctifs, la reconfiguration ou d'autres mesures d'atténuation.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.2e	Utilisez des mécanismes automatisés pour détecter les composants système mal configurés ou non autorisés ; après détection , [Sélection (un ou plusieurs) : retirez les composants; placez les composants dans un réseau de quarantaine ou de mise à jour] afin de faciliter l'application de correctifs, la reconfiguration ou d'autres mesures d'atténuation.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.2e	Utilisez des mécanismes automatisés pour détecter les composants système mal configurés ou non autorisés ; après détection , [Sélection (un ou plusieurs) : retirez les composants; placez les composants dans un réseau de quarantaine ou de mise à jour] afin de faciliter l'application de correctifs, la reconfiguration ou d'autres mesures d'atténuation.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.3e	Utilisez des outils de découverte et de gestion automatisés pour maintenir un inventaire complet up-to-date, précis et facilement disponible des composants du système.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.3e	Utilisez des outils de découverte et de gestion automatis és pour maintenir un inventaire complet up-to-date, précis et facilement disponibl e des composants du système.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.3e	Utilisez des outils de découverte et de gestion automatisés pour maintenir un inventaire complet up-to-date, précis et facilement disponible des composants du système.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4.3e	Utilisez des outils de découverte et de gestion automatis és pour maintenir un inventaire complet up-to-date, précis et facilement disponibl e des composants du système.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.
3.4.3e	Utilisez des outils de découverte et de gestion automatis és pour maintenir un inventaire complet up-to-date, précis et facilement disponibl e des composants du système.	vpc-network-acl-un used-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2e	Utilisez des mécanismes automatisés pour la création, la protection, la rotation et la gestion des mots de passe pour les systèmes et les composants système qui ne prennent pas en charge l'authentification multifactorielle ou la gestion de comptes complexe.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2e	Utilisez des mécanismes automatisés pour la création, la protection, la rotation et la gestion des mots de passe pour les systèmes et les composants système qui ne prennent pas en charge l'authentification multifactorielle ou la gestion de comptes complexe.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
3.5.2e	Utilisez des mécanismes automatisés pour la création, la protection, la rotation et la gestion des mots de passe pour les systèmes et les composants système qui ne prennent pas en charge l'authentification multifactorielle ou la gestion de comptes complexe.	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2e	Utilisez des mécanismes automatisés pour la création, la protection, la rotation et la gestion des mots de passe pour les systèmes et les composants système qui ne prennent pas en charge l'authentification multifactorielle ou la gestion de comptes complexe.	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.11.1e	Utilisez [Attribution : sources de renseignements sur les menaces définies par l'organisation] dans le cadre d'une évaluation des risques afin d'orienter et d'éclairer le développement des systèmes, des architectures de sécurité, de la sélection des solutions de sécurité, de la surveillance, de la détection des menaces et des activités de réponse et de reprise de l'organisation.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.11.2e	Menez des activités de détection des cybermenaces [Sélection (un ou plusieurs) : [Attribution : fréquence définie par l'organisation] ; [Attribution : événement défini par l'organisation]] pour rechercher des indicateurs de compromission dans [Attribution : systèmes définis par l'organisation] et détecter, suivre et neutraliser les menaces qui échappent aux contrôles existants.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.11.5e	Évaluez l'efficacité des solutions de sécurité [Attribution : fréquence définie par l'organisation] pour faire face aux risques anticipés pesant sur les systèmes de l'organisation et sur l'organisation, en vous appuyant sur les informations actuelles et accumulées sur les menaces.	annual-risk-assessment-performed (vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	nacl-no-unrestricted-ssh-rdp	L'accès aux ports d'administration des serveurs distants figurant dans vos listes de contrôle d'accès au réseau (NACL), tels que le port 22 (SSH) et le port 3389 (RDP), ne doit pas être accessible au public, car cela pourrait permettre un accès imprévu à des ressources au sein de votre VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.13.4e	Utilisez [Sélection : (un ou plusieurs) : [Attribution : techniques d'isolation physique définies par l'organisation] ; [Attribution : techniques d'isolation logique définies par l'organisation]] dans les systèmes et les composants système de l'organisation.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.1e	Vérifiez l'intégrité de [Attribution : logiciel essentiel ou stratégique pour la sécurité défini par l'organisation] à l'aide de mécanismes de confiance ou de signatures chiffrées.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2e	Surveillez en permanence les systèmes de l'organisation et leurs composant s afin de détecter tout comportement anormal ou suspect.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2e	Surveillez en permanence les systèmes de l'organisation et leurs composant s afin de détecter tout comportement anormal ou suspect.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2e	Surveillez en permanence les systèmes de l'organisation et leurs composants afin de détecter tout comportement anormal ou suspect.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2e	Surveillez en permanence les systèmes de l'organisation et leurs composant s afin de détecter tout comportement anormal ou suspect.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2e	Surveillez en permanence les systèmes de l'organisation et leurs composant s afin de détecter tout comportement anormal ou suspect.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2e	Surveillez en permanence les systèmes de l'organisation et leurs composants afin de détecter tout comportement anormal ou suspect.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.2e	Surveillez en permanence les systèmes de l'organisation et leurs composant s afin de détecter tout comportement anormal ou suspect.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.6e	Utilisez les informations sur les indicateurs de menace et les mesures d'atténuation efficaces obtenues auprès de [Attribution : organisations externes définies par l'organisation] pour orienter et informer la détection des intrusions et des menaces.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.7e	Vérifiez l'exactitude des [Attribution : composants logiciels , microprogrammes et matériels essentiels ou stratégiques pour la sécurité définis par l'organisation] à l'aide de [Attribution : méthodes ou techniques de vérification définies par l'organisation].	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.7e	Vérifiez l'exactitude des [Attribution : composants logiciels , microprogrammes et matériels essentiels ou stratégiques pour la sécurité définis par l'organisation] à l'aide de [Attribution : méthodes ou techniques de vérification définies par l'organisation].	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.7e	Vérifiez l'exactitude des [Attribution : composants logiciels , microprogrammes et matériels essentiels ou stratégiques pour la sécurité définis par l'organisation] à l'aide de [Attribution : méthodes ou techniques de vérification définies par l'organisation].	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.7e	Vérifiez l'exactitude des [Attribution : composants logiciels , microprogrammes et matériels essentiels ou stratégiques pour la sécurité définis par l'organisation] à l'aide de [Attribution : méthodes ou techniques de vérification définies par l'organisation].	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.14.7e	Vérifiez l'exactitude des [Attribution : composants logiciels , microprogrammes et matériels essentiels ou stratégiques pour la sécurité définis par l'organisation] à l'aide de [Attribut ion : méthodes ou techniques de vérificat ion définies par l'organisation].	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur . L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégri té et de la sécurité des images stockées.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST 800 172.

Bonnes pratiques de fonctionnement pour NIST 800 181

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le NIST 800 181 et les règles de configuration AWS gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NIST 800 181. Un contrôle NIST 800 181 peut être

associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
T0008	Analysez et planifiez les modifications prévues des besoins en matière de capacité de données.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	opensearch-encrypted-at-rest	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon Elasticsearch Service (Amazon ES).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0017	Appliquez les principes de l'architecture de sécurité orientée services pour répondre aux exigences de l'organisation en matière de confidentialité, d'intégrité et de disponibilité.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0024	Collectez et tenez à jour les données nécessaires à l'établissement des rapports sur la cybersécurité des systèmes.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0042	Coordonnez-vous avec les analystes de cyberdéfense pour gérer et administrer la mise à jour des règles et des signatures (par exemple, les systèmes de détection /protection contre les intrusions, les antivirus et les listes noires de contenu) pour les applicati ons de cyberdéfense spécialisées.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0047	Mettez en corrélati on les données relatives aux incidents afin d'identifier les vulnérabilités spécifiques et de formuler des recommandations permettant de les corriger rapidement.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences approprié es en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/resta uration du système.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences approprié es en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/resta uration du système.	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences approprié es en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/resta uration du système.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences approprié es en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/resta uration du système.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences approprié es en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/resta uration du système.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences approprié es en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/resta uration du système.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
T0051	Définissez les niveaux appropriés de disponibilité du système selon les fonctions critiques du système et veillez à ce que les exigences du système définissent les exigences appropriées en matière de reprise après sinistre et de continuité des opérations, notamment les exigences en matière de basculement ou de site alternatif, de sauvegarde et de support matériel pour la récupération/restauration du système.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0065	Élaborez et mettez en œuvre des procédures de sauvegarde et de récupération du réseau.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0070	Élaborez des plans de reprise après sinistre et de continuité des opérations pour les systèmes en cours de développement et veillez à ce qu'ils soient testés avant d'être introduits dans un environnement de production.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0086	Assurez-vous que l'application des correctifs de sécurité pour les produits commerciaux intégrés dans la conception du système respecte les délais prescrits par l'autorité de gestion pour l'environnement opérationnel prévu.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0086	Assurez-vous que l'application des correctifs de sécurité pour les produits commerciaux intégrés dans la conception du système respecte les délais prescrits par l'autorité de gestion pour l'environnement opérationnel prévu.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0086	Assurez-vous que l'application des correctifs de sécurité pour les produits commerciaux intégrés dans la conception du système respecte les délais prescrits par l'autorité de gestion pour l'environnement opérationnel prévu.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0086	Assurez-vous que l'application des correctifs de sécurité pour les produits commerciaux intégrés dans la conception du système respecte les délais prescrits par l'autorité de gestion pour l'environnement opérationnel prévu.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0110	Identifiez et/ou déterminez si un incident de sécurité constitue une violation de la loi nécessitant une action juridique spécifique.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0110	Identifiez et/ou déterminez si un incident de sécurité constitue une violation de la loi nécessitant une action juridique spécifique.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0110	Identifiez et/ou déterminez si un incident de sécurité constitue une violation de la loi nécessitant une action juridique spécifique.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0128	Intégrez des capacités automatisées de mise à jour ou de correction des logiciels du système lorsque cela est possible et élaborez des processus et des procédures pour la mise à jour et la correction manuelles des logiciels du système en fonction des exigences actuelles et prévues en matière de délais de correction pour l'environnement opérationnel du système.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0128	Intégrez des capacités automatisées de mise à jour ou de correction des logiciels du système lorsque cela est possible et élaborez des processus et des procédures pour la mise à jour et la correction manuelles des logiciels du système en fonction des exigences actuelles et prévues en matière de délais de correction pour l'environnement opérationnel du système.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0128	Intégrez des capacités automatisées de mise à jour ou de correction des logiciels du système lorsque cela est possible et élaborez des processus et des procédures pour la mise à jour et la correction manuelles des logiciels du système en fonction des exigences actuelles et prévues en matière de délais de correction pour l'environnement opérationnel du système.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0128	Intégrez des capacités automatisées de mise à jour ou de correction des logiciels du système lorsque cela est possible et élaborez des processus et des procédures pour la mise à jour et la correction manuelles des logiciels du système en fonction des exigences actuelles et prévues en matière de délais de correction pour l'environnement opérationnel du système.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informati ons administratives sur chaque principal.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon Elasticsearch Service (Amazon ES) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon ES au sein d'un réseau Amazon VPC permet une communica tion sécurisée entre Amazon ES et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0144	Gérez les comptes, les droits réseau et l'accès aux systèmes et aux équipements.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0151	Surveillez et évaluez l'efficacité des mesures de protection de l'entreprise en matière de cybersécurité afin de vous assurer qu'elles offrent le niveau de protection voulu.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0151	Surveillez et évaluez l'efficacité des mesures de protection de l'entreprise en matière de cybersécurité afin de vous assurer qu'elles offrent le niveau de protection voulu.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0151	Surveillez et évaluez l'efficacité des mesures de protection de l'entreprise en matière de cybersécurité afin de vous assurer qu'elles offrent le niveau de protection voulu.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
T0152	Surveillez et gérez les bases de données afin de garantir des performances optimales.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0153	Surveillez la capacité et les performances du réseau.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0153	Surveillez la capacité et les performances du réseau.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
T0153	Surveillez la capacité et les performances du réseau.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0153	Surveillez la capacité et les performances du réseau.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissa nces.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0154	Surveillez et signalez l'utilisation des actifs et des ressources de gestion des connaissances.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0156	Supervisez la gestion de la configuration et formulez des recommandations à ce sujet.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0160	Corrigez les vulnérabilités du réseau afin de garantir la protection des informations contre des tiers.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0160	Corrigez les vulnérabilités du réseau afin de garantir la protection des informations contre des tiers.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0160	Corrigez les vulnérabilités du réseau afin de garantir la protection des informations contre des tiers.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0162	Effectuez la sauvegarde et la restauration des bases de données pour garantir l'intégrité des données.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0166	Mettez en corrélation les événements à l'aide d'informations recueillies auprès de diverses sources au sein de l'entreprise afin d'obtenir une meilleure visibilité de la situation et de déterminer l'efficacité d'une attaque observée.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0168	Effectuez une comparaison de hachage par rapport à une base de données établie.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon Elasticsearch Service (Amazon ES) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon ES au sein d'un réseau Amazon VPC permet une communica tion sécurisée entre Amazon ES et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0195	Fournissez un flux géré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0215	Identifiez une éventuelle violation de la sécurité et prenez les mesures appropriées pour signaler l'incident, le cas échéant.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0244	Vérifiez que les mesures de sécurité des logiciels d'application, des réseaux et des systèmes sont mises en œuvre comme prévu, documentez tout écart et recommandez les mesures à prendre pour le corriger.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0244	Vérifiez que les mesures de sécurité des logiciels d'application, des réseaux et des systèmes sont mises en œuvre comme prévu, documentez tout écart et recommandez les mesures à prendre pour le corriger.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0244	Vérifiez que les mesures de sécurité des logiciels d'application, des réseaux et des systèmes sont mises en œuvre comme prévu, documentez tout écart et recommandez les mesures à prendre pour le corriger.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0258	Détectez, identifiez et alertez rapidemen t en cas d'attaques/ intrusions, d'activit és anormales et d'utilisations abusives, et distingue z ces incidents et événements des activités ordinaires.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0259	Utilisez des outils de cyberdéfense pour surveiller et analyser en permanence l'activité du système afin d'identifier les activités malveillantes.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon Elasticsearch Service (Amazon ES) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon ES au sein d'un réseau Amazon VPC permet une communica tion sécurisée entre Amazon ES et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0262	Utilisez des defense-in-depth principes et des pratiques approuvés (par exemple, defense-in-multiple lieux, défenses en couches, robustesse de la sécurité).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon Elasticsearch Service (Amazon ES) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon ES au sein d'un réseau Amazon VPC permet une communication sécurisée entre Amazon ES et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0284	Concevez et élaborez de nouveaux ou nouvelles outils/technologies lié(e)s à la cybersécurité.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0306	Prend en charge la gestion des incidents, la gestion des niveaux de service, la gestion des modifications, la gestion des versions, la gestion de la continuité et la gestion de la disponibilité des bases de données et des systèmes de gestion des données.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0306	Prend en charge la gestion des incidents, la gestion des niveaux de service, la gestion des modifications, la gestion des versions, la gestion de la continuité et la gestion de la disponibilité des bases de données et des systèmes de gestion des données.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0306	Prend en charge la gestion des incidents, la gestion des niveaux de service, la gestion des modifications, la gestion des versions, la gestion de la continuité et la gestion de la disponibilité des bases de données et des systèmes de gestion des données.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0314	Élaborez un contexte de sécurité des systèmes, un concept prélimina ire de sécurité du système (CONOPS) et définissez les exigences de base en matière de sécurité du système conformém ent aux exigences applicables en matière de cybersécu rité.	ec2-instance-manag ed-by-systems-mana ger	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillée s, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0314	Élaborez un contexte de sécurité des systèmes, un concept prélimina ire de sécurité du système (CONOPS) et définissez les exigences de base en matière de sécurité du système conformém ent aux exigences applicables en matière de cybersécu rité.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des référence s pour les niveaux de correctifs du système d'exploitation, les installations logiciell es, les configura tions d'application et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0314	Élaborez un contexte de sécurité des systèmes, un concept prélimina ire de sécurité du système (CONOPS) et définissez les exigences de base en matière de sécurité du système conformém ent aux exigences applicables en matière de cybersécu rité.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformém ent aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0314	Élaborez un contexte de sécurité des systèmes, un concept prélimina ire de sécurité du système (CONOPS) et définissez les exigences de base en matière de sécurité du système conformém ent aux exigences applicables en matière de cybersécu rité.	ec2-volume-inuse-c heck	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'un e instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0314	Élaborez un contexte de sécurité des systèmes, un concept prélimina ire de sécurité du système (CONOPS) et définissez les exigences de base en matière de sécurité du système conformém ent aux exigences applicables en matière de cybersécu rité.	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0314	Élaborez un contexte de sécurité des systèmes, un concept prélimina ire de sécurité du système (CONOPS) et définissez les exigences de base en matière de sécurité du système conformém ent aux exigences applicables en matière de cybersécu rité.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0333	Effectuez des analyses et générez des rapports sur les tendances en matière de cyberdéfense.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0333	Effectuez des analyses et générez des rapports sur les tendances en matière de cyberdéfense.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0347	Évaluez la validité des données sources et des résultats qui en découlent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0358	Concevez et développez des fonctionnalités d'administration et de gestion du système pour les utilisateurs qui disposent d'un accès privilégié.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organis ation.	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0376	Établissez des programmes de gestion des effectifs cyber, dotez-les de ressources, mettez-les en œuvre et évaluez-les conformément aux exigences de l'organisation.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
T0416	Permettez l'utilisation d'applications à clé publique en exploitant les bibliothèques d'infrastructure à clé publique (PKI) existantes et en incorporant des fonctionnalités de gestion et de chiffrement des certificats, le cas échéant.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparation des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authentifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification. Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0421	Gérez l'indexation/le catalogage, le stockage et l'accès à des connaissances organisationnelles explicites (par exemple, des documents papier, des fichiers numériques).	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informati ons administratives sur chaque principal.
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon Elasticsearch Service (Amazon ES) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon ES au sein d'un réseau Amazon VPC permet une communica tion sécurisée entre Amazon ES et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0475	Évaluez les contrôles d'accès adéquats sur la base des principes du moindre privilège et need-to-know.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0489	Mettez en œuvre des mesures de sécurité du système conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0491	Installez et configurez le matériel, les logiciels et les équipements périphériques pour les utilisateurs du système conformément aux normes de l'organisation.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0491	Installez et configurez le matériel, les logiciels et les équipements périphériques pour les utilisateurs du système conformément aux normes de l'organisation.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0491	Installez et configurez le matériel, les logiciels et les équipements périphériques pour les utilisateurs du système conformément aux normes de l'organisation.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0503	Surveillez les sources de données externes (par exemple, les sites des fournisseurs de cyberdéfense, les équipes d'intervention en cas d'urgence informatique, Security Focus) afin de maintenir l'actuali té des menaces de cyberdéfense et de déterminer les problèmes de sécurité susceptibles d'avoir un impact sur l'entrepr ise.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
T0509	Effectuez une évaluation des risques en matière de sécurité de l'information.	annual-risk-assess ment-performed (vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisat ion. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifié s sur une organisat ion.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon Elasticsearch Service est activé. ode-to-no de Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	opensearch-encrypted-at-rest	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon Elasticsearch Service (Amazon ES).
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon Elasticsearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	elasticsearch-encrypted-at-rest	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon Elasticsearch Service (Amazon ES).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0553	Appliquez des fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les opportunités d'exploitation.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
T0557	Intégrez les fonctions de gestion des clés liées au cyberespace.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés ont fait l'objet d'une rotation une fois la fin de leur période de chiffrement atteinte.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0557	Intégrez les fonctions de gestion des clés liées au cyberespace.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0576	Évaluez les renseignements provenant de toutes les sources et recommandez des cibles destinées à soutenir les objectifs des cyber-opérations.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon Elasticsearch Service (Amazon ES) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon ES au sein d'un réseau Amazon VPC permet une communica tion sécurisée entre Amazon ES et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon Elasticsearch Service (Amazon ES) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon ES au sein d'un réseau Amazon VPC permet une communica tion sécurisée entre Amazon ES et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0609	Permettez l'accès aux réseaux informatiques et numériques sans fil.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0616	Effectuez des repérages du réseau et des analyses de vulnérabilité des systèmes au sein d'un réseau.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0686	Identifiez les vulnérabilités aux menaces.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0686	Identifiez les vulnérabilités aux menaces.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	cw-loggroup-retent ion-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisant e pour faciliter le dépannage et les enquêtes judiciair es. Le manque de données disponibl es dans les journaux d'événements passés complique la reconstit ution et l'identification des événement s potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés dans les domaines du service Amazon Elasticse arch et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservat ion et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	rds-enhanced-monit oring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibi lité d'Amazon RDS. Vous disposez ainsi d'une visibilit é détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploieme nt multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	wafv2-logging-enab led	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informati ons détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspon dait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrast ructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibi lité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournisse nt un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0706	Recueillez des informations sur les réseaux à l'aide de techniques tradition nelles et alternatives (par exemple, analyse des réseaux sociaux, chaîne d'appels, analyse du trafic).	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0777	Établissez le profil des administrateurs de réseaux ou de systèmes et de leurs activités.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0805	Signalez les événements et les intrusions réseau importants provenant de renseignements.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informati ons des consommat eurs	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informati ons des consommat eurs	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0877	Travaillez en coopération avec les unités compétentes de l'organisation pour superviser les droits d'accès aux informations des consommateurs	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0935	Effectuez une évaluation des risques en matière de sécurité de l'information.	annual-risk-assessment-performed (vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référencer le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
T0960	Surveillez les modifications apportées à un système et à son environnement de fonctionnement.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0992	Déterminez comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
T0993	Mettez en place des outils de surveillance continue et des procédures de contrôle des accès aux technologies.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST 800 181.

Bonnes pratiques de fonctionnement pour NIST 1800 25

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas

conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le NIST 1800-25 et les règles de AWS configuration gérées. Chacune AWS Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NIST 1800-25. Un contrôle NIST 1800-25 peut être associé à plusieurs règles. AWS Config Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			informations sur votre environnement.
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
PR.AC-1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisate urs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourci r la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configur ation par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
PR.AC-3	L'accès à distance est géré.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-3	L'accès à distance est géré.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.AC-3	L'accès à distance est géré.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-3	L'accès à distance est géré.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
PR.AC-3	L'accès à distance est géré.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-3	L'accès à distance est géré.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-3	L'accès à distance est géré.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informati ons administratives sur chaque principal.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
PR.DS-1	D ata-at-rest est protégé	rds-snapshot-encry pted	Assurez-vous que le chiffrement est activé pour vos instantan és Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
PR.DS-1	D ata-at-rest est protégé	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
PR.DS-1	D ata-at-rest est protégé	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
PR.DS-1	D ata-at-rest est protégé	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
PR.DS-1	D ata-at-rest est protégé	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
PR.DS-1	D ata-at-rest est protégé	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
PR.DS-1	D ata-at-rest est protégé	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
PR.DS-2	D ata-in-transit est protégé	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
PR.DS-2	D ata-in-transit est protégé	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
PR.DS-2	D ata-in-transit est protégé	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-6	Les mécanismes de contrôle d'intégrité sont utilisés pour vérifier l'intégrité des logiciels, des microprogrammes et des informations	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-6	Les mécanismes de contrôle d'intégrité sont utilisés pour vérifier l'intégrité des logiciels, des microprogrammes et des informations	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-3	Des processus de contrôle des modifications de configuration sont en place	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-3	Des processus de contrôle des modificat ions de configuration sont en place	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-9	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de récupération (récupération après incident et reprise après sinistre) sont en place et gérés.	response-plan-exists-maintained (Vérification du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsable. Le fait de disposer de plans de réponse mis à jour et officiellement documentés permet de s'assurer que le personnel d'intervention comprend les rôles, les responsabilités et les processus à suivre en cas d'incident.
PR.IP-10	Les plans de réponse et de récupération sont testés.	response-plan-tested (Vérification du processus)	Assurez-vous que les plans de réponse et de reprise sont testés. Cela peut vous aider à comprendre si votre plan sera efficace en cas d'incident et si des lacunes doivent être corrigées ou des mises à jour effectuées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-12	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre.	vuln-management-plan-exists (Vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement. Cela peut inclure des outils de gestion des vulnérabilités, la cadence d'analyse de l'environnement, les rôles et les responsabilités.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-12	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-12	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-12	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.MA-2	La maintenance à distance des actifs de l'organisation est approuvée, consignée et effectuée de manière à empêcher tout accès non autorisé	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
PR.MA-2	La maintenance à distance des actifs de l'organisation est approuvée, consignée et effectuée de manière à empêcher tout accès non autorisé	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
PR.PT-1	Les réseaux de communication et de contrôle sont protégés	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	guardduty-enabled-centralized	Amazon GuardDuty peut aider à surveille r et à détecter les événement s de cybersécu rité potentiels en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionn alité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-8	Des analyses de vulnérabilité sont effectuées.	vuln-scans-performed (Vérification du processus)	Assurez-vous que des analyses de vulnérabilité sont effectuées conformément à vos exigences de conformité. La cadence d'analyse, les outils utilisés et l'utilisation des résultats doivent être définis par votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.MI-3	Les vulnérabilités nouvellement identifiées sont atténuées ou documentées en tant que risques acceptés.	vuln-mitigated-accepted (Vérification du processus)	Assurez-vous que les vulnérabilités nouvellement identifiées sont corrigées ou documentées en tant que risques acceptés. Des services tels que AWS Security Hub, Amazon Guard Duty, Amazon Inspector et AWS Config peuvent vous aider à identifier les vulnérabilités de votre environnement. Les vulnérabilités doivent être corrigées ou considérées comme des risques conformément aux exigences de conformité de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.MI-3	Les vulnérabilités nouvellement identifiées sont atténuées ou documentées en tant que risques acceptés	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST 1800 25.

Bonnes pratiques de fonctionnement pour NIST CSF

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou

d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le NIST Cyber Security Framework (CSF) et les règles de AWS configuration gérées. Chaque AWS Config règle s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NIST CSF. Un contrôle NIST CSF peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	utilisateurs et les systèmes est établie et gérée		d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-1	Une référence des opérations réseau et des flux de données prévus pour les utilisateurs et les systèmes est établie et gérée	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-2	Les événements détectés sont analysés pour comprendre les cibles et les méthodes d'attaque	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-2	Les événement s détectés sont analysés pour comprendre les cibles et les méthodes d'attaque	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-3	Les données d'événements sont collectées et mises en corrélation à partir de plusieurs sources et capteurs	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
DE.AE-4	L'impact des événements est déterminé	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-4	L'impact des événements est déterminé	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-4	L'impact des événements est déterminé	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-4	L'impact des événements est déterminé	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-4	L'impact des événements est déterminé	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-4	L'impact des événements est déterminé	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
DE.AE-4	L'impact des événements est déterminé	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.AE-4	L'impact des événements est déterminé	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-1	Le réseau est surveillé afin de détecter d'éventuels événements liés à la cybersécurité	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.
DE.CM-3	L'activité du personnel est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-3	L'activité du personnel est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-3	L'activité du personnel est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-3	L'activité du personnel est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
DE.CM-3	L'activité du personnel est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-3	L'activité du personnel est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-4	Du code malveillant est détecté	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-4	Du code malveillant est détecté	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-5	Du code mobile non autorisé est détecté	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.
DE.CM-5	Du code mobile non autorisé est détecté	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-5	Du code mobile non autorisé est détecté	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-5	Du code mobile non autorisé est détecté	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-5	Du code mobile non autorisé est détecté	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-5	Du code mobile non autorisé est détecté	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-6	L'activité des fournisseurs de services externes est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-6	L'activité des fournisseurs de services externes est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-6	L'activité des fournisseurs de services externes est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-6	L'activité des fournisseurs de services externes est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
DE.CM-6	L'activité des fournisseurs de services externes est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-6	L'activité des fournisseurs de services externes est surveillée afin de détecter d'éventuels événements liés à la cybersécurité	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.CM-7	La surveillance du personnel, des connexions, des appareils et des logiciels non autorisés est assurée	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.DP-4	Les informations relatives à la détection des événements sont communiquées	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.
DE.DP-4	Les informations relatives à la détection des événements sont communiquées	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.DP-4	Les informations relatives à la détection des événements sont communiquées	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.DP-4	Les informations relatives à la détection des événements sont communiquées	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.DP-4	Les informations relatives à la détection des événements sont communiquées	s3-event-notifications-enabled	Les notifications d'événements Amazon S3 peuvent alerter le personnel concerné de toute modification accidentelle ou intentionnelle des objets de votre compartiment. Voici quelques exemples d'alertes : création d'un nouvel objet, suppression d'un objet, restauration d'un objet, objets perdus ou répliqués.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.DP-4	Les informations relatives à la détection des événements sont communiquées	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.DP-4	Les informations relatives à la détection des événements sont communiquées	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
DE.DP-5	Les processus de détection sont continuellement améliorés	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.
ID.AM-2	Les plateformes logicielles et les applications au sein de l'organisation sont inventoriées	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-3	La communication organisationnelle et les flux de données sont mappés	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
ID.AM-3	La communication organisationnelle et les flux de données sont mappés	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-3	La communication organisationnelle et les flux de données sont mappés	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-3	La communication organisationnelle et les flux de données sont mappés	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-3	La communication organisationnelle et les flux de données sont mappés	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-3	La communication organisationnelle et les flux de données sont mappés	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.AM-3	La communication organisationnelle et les flux de données sont mappés	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiels sont établies pour tous les états d'exploitation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opérations normales)	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiels sont établies pour tous les états d'exploitation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opérations normales)	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiels sont établies pour tous les états d'exploitation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opérations normales)	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiels sont établies pour tous les états d'exploitation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opérations normales)	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiels sont établies pour tous les états d'exploitation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opérations normales)	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiel s sont établies pour tous les états d'exploit ation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opération s normales)	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.BE-5	Les exigences de résilience pour soutenir la prestation de services essentiels sont établies pour tous les états d'exploitation (par exemple en cas de contrainte ou d'attaque, pendant le rétablissement, pendant les opérations normales)	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-1	Les vulnérabilités des ressources sont identifiées et documentées	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-2	Les renseignements sur les cybermena ces proviennent de forums et de sources de partage d'informa tions	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-3	Les menaces, internes et externes, sont identifiées et documentées	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-3	Les menaces, internes et externes, sont identifiées et documentées	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.SC-4	Les fournisseurs et les partenaires tiers sont régulière ment évalués à l'aide d'audits, de résultats de tests ou d'autres formes d'évaluat ion afin de vérifier qu'ils respectent leurs obligations contractu elles.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.SC-4	Les fournisseurs et les partenaires tiers sont régulière ment évalués à l'aide d'audits, de résultats de tests ou d'autres formes d'évaluat ion afin de vérifier qu'ils respectent leurs obligations contractu elles.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.SC-4	Les fournisseurs et les partenaires tiers sont régulièrement évalués à l'aide d'audits, de résultats de tests ou d'autres formes d'évaluation afin de vérifier qu'ils respectent leurs obligations contractuelles.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.SC-4	Les fournisseurs et les partenaires tiers sont régulière ment évalués à l'aide d'audits, de résultats de tests ou d'autres formes d'évaluat ion afin de vérifier qu'ils respectent leurs obligations contractu elles.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les appareils, les utilisateurs et les processus autorisés	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-3	L'accès à distance est géré.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.AC-3	L'accès à distance est géré.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-3	L'accès à distance est géré.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
PR.AC-3	L'accès à distance est géré.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-3	L'accès à distance est géré.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-3	L'accès à distance est géré.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-3	L'accès à distance est géré.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-instance-profile-attached	Les profils d'instanc e EC2 transmett ent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-6	Les identités sont prouvées, liées à des informations d'identif ication et affirmées dans des interactions	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-6	Les identités sont prouvées, liées à des informations d'identif ication et affirmées dans des interactions	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-7	Les utilisateurs, les appareils et les autres actifs sont authentif iés (par exemple, à facteur unique, à facteurs multiples) en fonction du risque de la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et autres risques organisat ionnels)	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-7	Les utilisateurs, les appareils et les autres actifs sont authentif iés (par exemple, à facteur unique, à facteurs multiples) en fonction du risque de la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et autres risques organisat ionnels)	iam-user-mfa-enabled	Activez cette règle pour limiter l'accès aux ressources dans le Cloud AWS . Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-7	Les utilisateurs, les appareils et les autres actifs sont authentif iés (par exemple, à facteur unique, à facteurs multiples) en fonction du risque de la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et autres risques organisat ionnels)	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-7	Les utilisateurs, les appareils et les autres actifs sont authentif iés (par exemple, à facteur unique, à facteurs multiples) en fonction du risque de la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et autres risques organisat ionnels)	root-account-hardw are-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémen taire de protection pour les informati ons d'identification de connexion En exigeant l'authent ification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-7	Les utilisateurs, les appareils et les autres actifs sont authentif iés (par exemple, à facteur unique, à facteurs multiples) en fonction du risque de la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et autres risques organisat ionnels)	root-account-mfa-e nabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisa teur root. L'utilisa teur root est l'utilisa teur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémen taire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'inciden ts de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AT-1	Tous les utilisate urs sont informés et formés	security-awareness -program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.
PR.DS-1	D ata-at-rest est protégé	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
PR.DS-1	D ata-at-rest est protégé	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
PR.DS-1	D ata-at-rest est protégé	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
PR.DS-1	D ata-at-rest est protégé	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
PR.DS-1	D ata-at-rest est protégé	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
PR.DS-1	D ata-at-rest est protégé	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
PR.DS-1	D ata-at-rest est protégé	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-1	D ata-at-rest est protégé	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
PR.DS-2	D ata-in-transit est protégé	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
PR.DS-2	D ata-in-transit est protégé	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
PR.DS-2	D ata-in-transit est protégé	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-2	D ata-in-transit est protégé	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-3	Les ressources sont officiellement gérées tout au long de la suppression, du transfert et de la disposition	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-3	Les ressources sont officiellement gérées tout au long de la suppression, du transfert et de la disposition	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-3	Les ressources sont officiellement gérées tout au long de la suppression, du transfert et de la disposition	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-4	Capacité adéquate pour garantir le maintien de la disponibilité	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild . AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codeb uild. Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-5	Des protections contre les fuites de données sont mises en œuvre	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-6	Les mécanismes de contrôle d'intégrité sont utilisés pour vérifier l'intégrité des logiciels, des microprogrammes et des informations	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-6	Les mécanismes de contrôle d'intégrité sont utilisés pour vérifier l'intégrité des logiciels, des microprogrammes et des informations	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-7	Le ou les environnements de développement et de test sont distincts de l'environnement de production	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-7	Le ou les environnements de développement et de test sont distincts de l'environnement de production	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-7	Le ou les environnements de développement et de test sont distincts de l'environnement de production	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-7	Le ou les environnements de développement et de test sont distincts de l'environnement de production	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-7	Le ou les environnements de développement et de test sont distincts de l'environnement de production	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-7	Le ou les environnements de développement et de test sont distincts de l'environnement de production	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-1	Une configuration de base des technologies de l'information et des systèmes de contrôle industriels est créée et maintenue en incorporant les principes de sécurité (par exemple le concept de moindre fonctionnalité)	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-2	Un cycle de vie de développement des systèmes est mis en œuvre pour gérer les systèmes	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-2	Un cycle de vie de développement des systèmes est mis en œuvre pour gérer les systèmes	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référenti el source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnel s ni d'identifiants de connexion dans les environnements de projet AWS Codeb uild. Utilisez OAuth au lieu de jetons d'accès personnel s ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-2	Un cycle de vie de développement des systèmes est mis en œuvre pour gérer les systèmes	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-3	Des processus de contrôle des modifications de configuration sont en place	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-3	Des processus de contrôle des modificat ions de configuration sont en place	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-4	Les sauvegardes des informations sont effectuées, maintenues et testées	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-7	Les processus de protection sont améliorés	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.
PR.IP-8	L'efficacité des technologies de protection est partagée	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.IP-8	L'efficacité des technologies de protection est partagée	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.IP-8	L'efficacité des technologies de protection est partagée	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.IP-8	L'efficacité des technologies de protection est partagée	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-8	L'efficacité des technologies de protection est partagée	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-12	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-12	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des références pour les niveaux de correctifs du système d'exploitation, les installations logicielles, les configurations d'application et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.IP-12	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.MA-2	La maintenance à distance des actifs de l'organisation est approuvée, consignée et effectuée de manière à empêcher tout accès non autorisé	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
PR.MA-2	La maintenance à distance des actifs de l'organisation est approuvée, consignée et effectuée de manière à empêcher tout accès non autorisé	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
PR.PT-1	Les réseaux de communication et de contrôle sont protégés	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les informations du compte AWS qui a accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-1	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-3	Le principe de moindre fonctionn alité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-4	Les réseaux de communication et de contrôle sont protégés	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	redshift-backup-en abled	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos clusters Amazon Redshift disposent d'instant anés automatisés. Lorsque les instantan és automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modificat ion des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-5	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RC.RP-1	Le plan de récupération est exécuté pendant ou après un incident de cybersécurité	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.AN-2	L'impact de l'incident est compris	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.MI-3	Les vulnérabilités nouvellement identifiées sont atténuées ou documentées en tant que risques acceptés	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
RS.RP-1	Le plan de réponse est exécuté pendant ou après un incident	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST CSF.

Bonnes pratiques de fonctionnement pour le cadre de confidentialité NIST v1.0

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre les règles du cadre de confidentialité NIST et les règles de configuration gérées par AWS . Chaque AWS Config règle s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles du NIST Privacy Framework. Un contrôle du NIST Privacy Framework peut être lié à plusieurs AWS Config règles. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CT.DM-P7	Des mécanisme s de transmiss	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.		Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	opensearch-node-to -node-encryption-c heck	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
CT.DM-P7	Des mécanisme s de transmiss ion des autorisat ions de traitemen t et des valeurs de données associées aux éléments de données sont établis et en place.	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	audit-log-policy-e xists (vérification du processus)	Établissez et maintenez une politique de gestion des journaux d'audit qui définit les exigences de votre organisat ion en matière de journalisation. Cela inclut, sans s'y limiter, l'examen et la conservation des journaux d'audit.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	cloudtrail-s3-data events-enabled	La collecte d'événeme nts de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique, et intègrent le principe de minimisation des données.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	cw-loggroup-retent ion-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisant e pour faciliter le dépannage et les enquêtes judiciair es. Le manque de données disponibl es dans les journaux d'événements passés complique la reconstit ution et l'identification des événement s potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique, et intègrent le principe de minimisation des données.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique, et intègrent le principe de minimisation des données.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique, et intègrent le principe de minimisation des données.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique, et intègrent le principe de minimisation des données.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminés, documentés, mis en œuvre et examinés conformément à la politique, et intègrent le principe de minimisation des données.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
CT.DM-P8	Les enregistrements d'audit/de journal sont déterminé s, documentés, mis en œuvre et examinés conformém ent à la politique, et intègrent le principe de minimisation des données.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
ID.DE-P2	Les parties à l'écosystème de traitement des données (par exemple, les fournisseurs de services, les clients, les partenaires, les fabricants de produits, les développeurs d'applications) sont identifiées, hiérarchisées et évaluées à l'aide d'un processus d'évaluation des risques liés à la confidentialité.	annual-risk-assessment-performed (vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identif ication sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
PR.AC-P1	Les identités et les informations d'identification sont émises, gérées, vérifiées, révoquées et auditées pour les personnes, les processus et les appareils autorisés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-P3	L'accès à distance est géré.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-P3	L'accès à distance est géré.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-P3	L'accès à distance est géré.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-P3	L'accès à distance est géré.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
PR.AC-P3	L'accès à distance est géré.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P3	L'accès à distance est géré.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiqu ement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévati on des privilèges inattendue lorsqu'un e définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P4	Les autorisations d'accès sont gérées et intègrent les principes du moindre privilège et de la séparation des tâches.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P5	L'intégrité du réseau est protégée (par exemple, ségrégation du réseau, segmentation du réseau).	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P6	Les personnes et les appareils sont vérifiés et liés à leurs informations d'identification, et authentifiés en fonction du risque lié à la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et les autres risques organisationnels).	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P6	Les personnes et les appareils sont vérifiés et liés à leurs informations d'identification, et authentifiés en fonction du risque lié à la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et les autres risques organisationnels).	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P6	Les personnes et les appareils sont vérifiés et liés à leurs informations d'identif ication, et authentif iés en fonction du risque lié à la transacti on (par exemple, les risques liés à la sécurité et à la confidentialité des individus et les autres risques organisat ionnels).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P6	Les personnes et les appareils sont vérifiés et liés à leurs informations d'identification, et authentifiés en fonction du risque lié à la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et les autres risques organisationnels).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.AC-P6	Les personnes et les appareils sont vérifiés et liés à leurs informations d'identification, et authentifiés en fonction du risque lié à la transaction (par exemple, les risques liés à la sécurité et à la confidentialité des individus et les autres risques organisationnels).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
PR.DS-P1	D ata-at-rest sont protégés.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
PR.DS-P1	D ata-at-rest sont protégés.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
PR.DS-P1	D ata-at-rest sont protégés.	elasticsearch-encr ypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
PR.DS-P1	D ata-at-rest sont protégés.	opensearch-encrypt ed-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.
PR.DS-P1	D ata-at-rest sont protégés.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
PR.DS-P1	D ata-at-rest sont protégés.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
PR.DS-P1	D ata-at-rest sont protégés.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P1	D ata-at-rest sont protégés.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
PR.DS-P2	D ata-in-transit sont protégés.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P2	D ata-in-transit sont protégés.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.
PR.DS-P2	D ata-in-transit sont protégés.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P2	D ata-in-transit sont protégés.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
PR.DS-P2	D ata-in-transit sont protégés.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P4	Capacité adéquate pour garantir le maintien de la disponibilité.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P5	Des protections contre les fuites de données sont mises en œuvre.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.DS-P6	Les mécanismes de contrôle d'intégrité sont utilisés pour vérifier l'intégrité des logiciels, des microprogrammes et des informations.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.MA-P2	La maintenance à distance des actifs de l'organisation est approuvée, consignée et effectuée de manière à empêcher tout accès non autorisé.	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.MA-P2	La maintenance à distance des actifs de l'organisation est approuvée, consignée et effectuée de manière à empêcher tout accès non autorisé.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P1	Une configuration de base des technologies de l'information est créée et maintenue en incorporant les principes de sécurité (par exemple, le concept de moindre fonctionnalité).	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
AT-1: PR.PO-P10	Un plan de gestion des vulnérabilités est élaboré et mis en œuvre.	vuln-management-plan-exists (vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P2	Des processus de contrôle des modifications de configuration sont en place.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P2	Des processus de contrôle des modificat ions de configuration sont en place.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P3	Les sauvegardes des informations sont effectuées, maintenues et testées.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activit é) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activit é) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activit é) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activit é) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activit é) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P7	Des plans de réponse (réponse aux incidents et continuité de l'activité) et des plans de reprise (reprise après incident et reprise après sinistre) sont en place et gérés.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PO-P8	Les plans de réponse et de récupération sont testés.	response-plan-tested (vérification du processus)	Assurez-vous que les plans de réponse et de reprise sont testés. Cela peut vous aider à comprendre si votre plan sera efficace en cas d'incident et si des lacunes doivent être corrigées ou des mises à jour effectuées.
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionn alité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P2	Le principe de moindre fonctionnalité est intégré en configurant les systèmes de manière à ne fournir que les fonctionnalités essentielles.	redshift-enhanced-vpc-routing-enabled	Le routage VPC amélioré oblige tout le trafic COPY et UNLOAD entre le cluster et les référentiels de données à passer par votre réseau Amazon VPC. Vous pouvez ensuite utiliser les fonctionnalités VPC, telles que les groupes de sécurité et les listes de contrôle d'accès réseau, pour sécuriser le trafic réseau. Vous pouvez également utiliser les journaux de flux VPC pour surveiller le trafic réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	lambda-function-pu blic-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiel lement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P3	Les réseaux de communication et de contrôle sont protégés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin qu'elle réponde automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	redshift-backup-en abled	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos clusters Amazon Redshift disposent d'instant anés automatisés. Lorsque les instantan és automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modificat ion des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	aurora-resources-p rotected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	backup-plan-min-fr equency-and-min-re tention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegard e est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e. Cette règle vous permet de définir les paramètres requiredFrequencyV alue (Config par défaut : 1), requiredR etentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restaurat ion Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressource s qui empêche la suppression de points de restaurat ion. L'utilisation d'une politique basée sur les ressource s pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	ec2-resources-prot ected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
PR.PT-P4	Des mécanisme s (par exemple, sécurité intégrée, équilibrage de charge, remplacement à chaud) sont mis en œuvre pour répondre aux exigences de résilience dans des situations normales et défavorables.	fsx-resources-prot ected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NIST Privacy Framework v1.0.

Bonnes pratiques de fonctionnement pour NYDFS 23

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou

d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de correspondance entre les exigences de cybersécurité du département des services financiers de l'État de New York (NYDFS) pour les sociétés de services financiers (23 NYCRR 500) et les règles de configuration gérées AWS . Chaque AWS Config règle s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles américains du NYDFS. Un contrôle US NYDFS 23 NYCRR 500 peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartiment Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouillage d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	beanstalk-enhanced-health-reporting-enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrastructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibilité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournissent un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02 (a)	(a) Programme de cybersécurité. Chaque entité concernée doit maintenir un programme de cybersécurité conçu pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information de l'entité concernée.	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	iam-password-policy	Les identités et les informations d'identif ication sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisat ionnelle. Ils respecten t ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundatio nal Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuell ement RequireUp percaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLo wercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonnées d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modificat ions apportées aux métadonnées des instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applicati ons Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromet tre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	api-gw-associated-with-waf	AWS Le WAF vous permet de configure r un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définisse z. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (2) utilisation d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisations ou autres actes malveillants non autorisés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(2)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (2) utilisati on d'une infrastructure défensive et mise en œuvre de politiques et de procédures pour protéger les systèmes d'information de l'entité concernée et les informations non publiques stockées sur ces systèmes d'information contre les accès, utilisati ons ou autres actes malveillants non autorisés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisate urs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	ec2-managedinstanc e-association-comp liance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisat ion. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploit ation, les installat ions de logiciels, les configurations d'applications et d'autres informati ons relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (3) détection des événements de cybersécurité.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement Multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (3) détection des événements de cybersécurité.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communica tion central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournisse nt des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (3) détection des événements de cybersécurité.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	vpc-flow-logs-enabled	Les journaux de flux VPC fournisse nt des informations détaillées sur le trafic IP circulant vers et depuis les interface s réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatc h ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génératio n fournissent des informations détaillée s sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (3) détection des événements de cybersécurité.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(3)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécu rité suivantes : (3) détection des événements de cybersécurité.	redshift-cluster-c onfiguration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalis ation des audits doit être activée pour fournir des informati ons sur les connexion s et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	redshift-backup-en abled	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos clusters Amazon Redshift disposent d'instant anés automatisés. Lorsque les instantan és automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modificat ion des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	dynamodb-pitr-enab led	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restaurat ion est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegard es continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	ebs-optimized-instance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluation des risques de l'entité concernée et conçu pour remplir les fonctions essentielles de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
500.02(b)(5)	(b) Le programme de cybersécurité doit être fondé sur l'évaluat ion des risques de l'entité concernée et conçu pour remplir les fonctions essentiel les de cybersécurité suivantes : (5) reprise après un événement de cybersécurité et rétablissement des opérations et des services normaux.	backup-recovery-po int-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressource s qui empêche la suppression de points de restaurat ion. L'utilisation d'une politique basée sur les ressource s pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,05	Le programme de cybersécurité de chaque entité concernée comprend une surveillance et des tests, élaborés conformément à l'évaluation des risques de l'entité concernée, destinés à évaluer l'efficac ité du programme de cybersécurité de l'entité concernée . La surveillance et les tests comprenne nt une surveillance continue ou des tests de pénétrati on périodiques et des évaluations de la vulnérabilité. En l'absence d'une surveillance continue efficace ou d'autres systèmes permettan t de détecter, en permanence, les modifications des systèmes d'informa tion susceptibles de créer ou d'indique r des vulnérabi	vuln-management-pl an-exists (vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiell ement définis pour remédier aux vulnérabilités dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	lités, les entités concernées doivent effectuer : (a) des tests de pénétration annuels des systèmes d'information de l'entité concernée déterminés chaque année en fonction des risques identifié s conformément à l'évaluation des risques ; et (b) des évaluations semestrie lles des vulnérabi lités de vulnérabi lité, notamment des analyses ou des examens systématiques des systèmes d'informa tion raisonnablement conçus pour identifie r les vulnérabilités de cybersécurité connues du public dans les systèmes d'information de l'entité concernée, en fonction de l'évaluat ion des risques.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06(b)	(b) Chaque entité concernée doit conserver les enregistrements requis par l'article 500.06 (a)(1) de la présente partie pendant au moins cinq ans et les enregistrements requis par l'article 500.06 (a)(2) de la présente partie pendant au moins trois ans.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.06 (a)	(a) Chaque entité concernée doit maintenir en toute sécurité des systèmes qui, dans la mesure applicable et en fonction de son évaluation des risques : (1) sont conçus pour reconstituer les transactions financières importantes suffisantes pour soutenir les opérations et obligations normales de l'entité concernée ; et (2) comprennent des pistes d'audit conçues pour détecter les événements de cybersécurité qui ont une probabilité raisonnable de nuire de manière significative à toute partie importante des opérations normales de l'entité concernée, et y répondre.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	ecs-task-definition-user-for-host-mode-check	Si une définition de tâche dispose de privilèges élevés, c'est parce que le client a spécifiquement opté pour ces configurations. Ce contrôle vérifie qu'il n'y a pas d'élévation des privilèges inattendue lorsqu'une définition de tâche a activé la mise en réseau de l'hôte, mais que le client n'a pas opté pour l'élévation des privilèges.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluat ion des risques de l'entité concernée , chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'informa tion qui donnent accès à des informati ons non publiques et doit revoir périodiqu ement ces privilèges d'accès.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluat ion des risques de l'entité concernée , chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'informa tion qui donnent accès à des informati ons non publiques et doit revoir périodiqu ement ces privilèges d'accès.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	lambda-inside-vpc	Déployez les fonctions AWS Lambda dans un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,07	Dans le cadre de son programme de cybersécurité, en fonction de l'évaluation des risques de l'entité concernée, chaque entité concernée doit limiter les privilèges d'accès des utilisateurs aux systèmes d'information qui donnent accès à des informations non publiques et doit revoir périodiquement ces privilèges d'accès.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.8 (a)	(a) Le programme de cybersécurité de chaque entité concernée doit comprendre des procédures écrites, des directives et des normes conçues pour garantir l'utilisation de pratiques de développement sécurisées pour les applications développées en interne et utilisées par l'entité concernée, ainsi que des procédures d'évaluation, de contrôle ou de test de la sécurité des applications développées en externe et utilisées par l'entité concernée dans le contexte de l'environnement technologique de l'entité concernée.	codebuild-project-envvar-awscred-check	Assurez-vous que les informations d'authentification AWS_ACCESS_KEY_ID et AWS_SECRET_ACCESS_KEY n'existent pas dans les environnements de projet Codebuild. AWS Ne stockez pas ces variables en clair. Le stockage de ces variables en clair entraîne une exposition involontaire des données et un accès non autorisé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.8 (a)	(a) Le programme de cybersécurité de chaque entité concernée doit comprendre des procédures écrites, des directives et des normes conçues pour garantir l'utilisation de pratiques de développement sécurisées pour les applications développées en interne et utilisées par l'entité concernée, ainsi que des procédures d'évaluation, de contrôle ou de test de la sécurité des applications développées en externe et utilisées par l'entité concernée dans le contexte de l'environnement technologique de l'entité concernée.	codebuild-project-source-repo-url-check	Assurez-vous que l'URL du référentiel source GitHub ou de Bitbucket ne contient pas de jetons d'accès personnels ni d'identifiants de connexion dans les environnements de projet AWS Codebuild. Utilisez OAuth au lieu de jetons d'accès personnels ou d'identifiants de connexion pour autoriser l'accès aux GitHub référentiels Bitbucket.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,09	(a) Chaque entité concernée doit procéder à une évaluation périodique des risques liés aux systèmes d'information de l'entité concernée, suffisante pour étayer la conception du programme de cybersécurité requis par la présente partie. Cette évaluation des risques est mise à jour lorsque cela est raisonnablement nécessaire pour tenir compte des modifications apportées aux systèmes d'information, aux informations non publiques ou aux opérations commerciales de l'entité concernée. L'évaluation des risques de l'entité concernée doit permettre de réviser les contrôles pour répondre aux développements technologiques et	annual-risk-assessment-performed (vérification du processus) >	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	à l'évolution des menaces et doit prendre en compte les risques particuliers des opérations commerciales de l'entité concernée liés à la cybersécurité, aux informations non publiques collectées ou stockées, aux systèmes d'information utilisés ainsi qu'à la disponibilité et à l'efficacité des contrôles visant à protéger les informations non publiques et les systèmes d'information.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,12	(a) Authentification multifactorielle. En fonction de son évaluation des risques, chaque entité concernée doit utiliser des contrôles efficaces, qui peuvent inclure l'authent ification multifact orielle ou l'authent ification basée sur les risques, pour se protéger contre l'accès non autorisé aux informations non publiques ou aux systèmes d'informa tion. (b) L'authent ification multifact orielle doit être utilisée pour toute personne accédant aux réseaux internes de l'entité concernée à partir d'un réseau externe, à moins que le RSSI de l'entité concernée n'ait approuvé par écrit l'utilisation de contrôles d'accès raisonnablement	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	équivalents ou plus sûrs.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,12	(a) Authentification multifactorielle. En fonction de son évaluation des risques, chaque entité concernée doit utiliser des contrôles efficaces, qui peuvent inclure l'authent ification multifact orielle ou l'authent ification basée sur les risques, pour se protéger contre l'accès non autorisé aux informations non publiques ou aux systèmes d'informa tion. (b) L'authent ification multifact orielle doit être utilisée pour toute personne accédant aux réseaux internes de l'entité concernée à partir d'un réseau externe, à moins que le RSSI de l'entité concernée n'ait approuvé par écrit l'utilisation de contrôles d'accès raisonnablement	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	équivalents ou plus sûrs.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,12	(a) Authentification multifactorielle. En fonction de son évaluation des risques, chaque entité concernée doit utiliser des contrôles efficaces, qui peuvent inclure l'authent ification multifact orielle ou l'authent ification basée sur les risques, pour se protéger contre l'accès non autorisé aux informations non publiques ou aux systèmes d'informa tion. (b) L'authent ification multifact orielle doit être utilisée pour toute personne accédant aux réseaux internes de l'entité concernée à partir d'un réseau externe, à moins que le RSSI de l'entité concernée n'ait approuvé par écrit l'utilisation de contrôles d'accès raisonnablement	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	équivalents ou plus sûrs.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,12	(a) Authentification multifactorielle. En fonction de son évaluation des risques, chaque entité concernée doit utiliser des contrôles efficaces, qui peuvent inclure l'authentification multifactorielle ou l'authentification basée sur les risques, pour se protéger contre l'accès non autorisé aux informations non publiques ou aux systèmes d'information. (b) L'authentification multifactorielle doit être utilisée pour toute personne accédant aux réseaux internes de l'entité concernée à partir d'un réseau externe, à moins que le RSSI de l'entité concernée n'ait approuvé par écrit l'utilisation de contrôles d'accès raisonnablement	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	équivalents ou plus sûrs.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,12	(a) Authentification multifactorielle. En fonction de son évaluation des risques, chaque entité concernée doit utiliser des contrôles efficaces, qui peuvent inclure l'authentification multifactorielle ou l'authentification basée sur les risques, pour se protéger contre l'accès non autorisé aux informations non publiques ou aux systèmes d'information. (b) L'authentification multifactorielle doit être utilisée pour toute personne accédant aux réseaux internes de l'entité concernée à partir d'un réseau externe, à moins que le RSSI de l'entité concernée n'ait approuvé par écrit l'utilisation de contrôles d'accès raisonnablement	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	équivalents ou plus sûrs.		
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	cloudwatch-alarm-action-check	Amazon CloudWatch émet une alerte lorsqu'un indicateur dépasse le seuil pour un certain nombre de périodes d'évaluation. L'alarme réalise une ou plusieurs actions en fonction de la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. Cette règle nécessite une valeur pour alarmActionRequired (Config Default : True), insufficientDataAction Required (Config Default : True), okActionRequired (Config Default : False). La valeur réelle doit refléter les actions d'alarme de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14 (a)	(a) mettre en œuvre des politiques, des procédures et des contrôles fondés sur les risques et conçus pour surveiller l'activité des utilisateurs autorisés et détecter l'accès, l'utilisation ou la modification non autorisés des informations non publiques par ces utilisateurs autorisés.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.14(b)	Dans le cadre de son programme de cybersécurité, chaque entité concernée doit : (b) dispenser régulièrement à l'ensemble du personnel une formation de sensibilisation à la cybersécurité mise à jour pour tenir compte des risques identifiés par l'entité concernée dans le cadre de son évaluation des risques.	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500.15 (a)	(a) Dans le cadre de son programme de cybersécurité, en fonction de son évaluation des risques, chaque entité concernée doit mettre en œuvre des contrôles, notamment le chiffrement, pour protéger les informations non publiques détenues ou transmises par l'entité concernée, à la fois en transit sur des réseaux externes et au repos.	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
500,16	(a) Dans le cadre de son programme de cybersécurité, chaque entité concernée doit établir un plan écrit de réponse aux incidents conçu pour répondre rapidemen t à tout événement de cybersécurité affectant matériell ement la confident ialité, l'intégrité ou la disponibi lité des systèmes d'information de l'entité concernée ou le fonctionnement continue de tout aspect de l'activité ou des opérations de l'entité concernée, et pour y remédier.	response-plan-exists-maintained (vérifica tion du processus)	Assurez-vous que des plans de réponse aux incidents sont établis, maintenus et distribués au personnel responsab le.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NYDFS 23.

Bonnes pratiques de fonctionnement pour NZISM

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas

conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le manuel de sécurité des informations (NZISM) de la version 3.6 du New Zealand Government Communications Security Bureau (GCSB) et les règles Managed AWS Config. Chaque règle de Config s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles NZISM. Un contrôle NZISM peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

Cet exemple de modèle de pack de conformité contient des mappages avec des contrôles au sein du cadre NZISM, qui fait partie intégrante du cadre des exigences de protection en matière de sécurité (Protective Security Requirements, PSR) qui définit les attentes du gouvernement néo-zélandais en matière de gestion de la sécurité du personnel, de l'information et de la sécurité physique.

Le NZISM est sous licence Creative Commons Attribution 4.0 New Zealand, disponible sur https://creativecommons.org/licenses/by/4.0/. Les informations sur les droits d'auteur sont disponibles dans le manuel de sécurité de l'information du NZISM néo-zélandais | Mentions légales, vie privée et droits d'auteur.

ID du contrôle	AWS Règle de configuration	Conseils
1149	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur

ID du contrôle	AWS Règle de configuration	Conseils
		et la version de l'application, ainsi que d'autres informations sur votre environnement.
1149	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
1149	ecs-containers-nonprivileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	AWS Règle de configuration	Conseils
1149	ecs-containers-readonly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque, car le système de fichiers de l'instance de conteneur ne peut être modifié que s'il dispose d'autorisations explicites de lecture et d'écriture.
1149	ec2- hardening-and-state-management (Vérification du processus)	Les processus renforcés de création d'images de serveurs EC2 et les associations de gestionnaires d'état sont configurés pour supprimer les composants et les services inutiles, et pour installer des logiciels contre les programmes malveillants et des agents de journalisation.

ID du contrôle	AWS Règle de configuration	Conseils
1661	cloudfront-default-root-object-configured	Ce contrôle vérifie si une CloudFront distribution Amazon est configurée pour renvoyer un objet spécifiqu e qui est l'objet racine par défaut. Le contrôle échoue si aucun objet racine par défaut n'est configuré pour la CloudFront distribution. Un utilisateur peut parfois demander l'URL racine de la distribution au lieu d'un objet de la distribution. Dans ce cas, la spécification d'un objet racine par défaut peut vous aider à éviter d'exposer le contenu de votre distribut ion web. Cette règle doit être appliquée dans la région us-east-1.
1667	acm-certificate-expiration-check	Assurez-vous que l'intégri té du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExp iration (valeur des meilleure s pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1667	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1841	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
1841	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
1841	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
1841	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
1847	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
1847	cloudfront-viewer-policy-https	Ce contrôle vérifie si une CloudFront distribution Amazon exige que les utilisateurs utilisent directement le protocole HTTPS ou si elle utilise la redirection. Le contrôle échoue s'il ViewerProtocolPolicy est défini sur allow-all pour defaultCacheBehavior ou pour CacheBehaviors. Le protocole HTTPS (TLS) peut être utilisé pour empêcher les attaquants potentiels d'utiliser person-in-the-middle des attaques similaires pour espionner ou manipuler le trafic réseau. Seules les connexions chiffrées via HTTPS (TLS) doivent être autorisées. Cette règle doit être appliquée dans la région us-east-1.

ID du contrôle	AWS Règle de configuration	Conseils
1847	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
1847	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
1847	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
1858	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
1893	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1893	federate-with-central-idp (Vérification du processus)	Les identités du personnel nécessitant un accès aux AWS ressources s'authent ifient auprès d'un IdP central AWS fédéré avec le SSO. L'IdP central bloque les utilisateurs du système après 3 tentatives de connexion infructueuses.
1946	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
1946	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
1998	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	AWS Règle de configuration	Conseils
1998	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
1998	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	AWS Règle de configuration	Conseils
2013	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
2013	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
2013	cloudfront-accesslogs-enabled	Ce contrôle vérifie si la journalisation des accès au serveur est activée sur les CloudFront distributions. Le contrôle échoue si la journalisation des accès n'est pas activée pour une distribution. CloudFront les journaux d'accès fournisse nt des informations détaillée s sur chaque demande d'utilisateur CloudFront reçue. Chaque journal contient des informations telles que la date et l'heure de réception de la demande, l'adresse IP de l'utilisateur qui a fait la demande, la source de la demande et le numéro de port de la demande formulée par l'utilisateur. Ces journaux sont utiles pour des applicati ons telles que les audits de sécurité et d'accès et les enquêtes judiciaires. Cette règle doit être appliquée dans la région us-east-1.

ID du contrôle	AWS Règle de configuration	Conseils
2013	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
2013	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
2013	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
2022	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
2022	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
2028	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
2082	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données. Une dérogation est possible pour les environnements de pré-production.
2082	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
2082	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
2082	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
2082	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
2082	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
2082	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
2082	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
2082	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2082	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
2082	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
2091	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2091	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
2091	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2598	elb-custom-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs ElasticLoadBalancer SSL classiques utilisent une politique de sécurité personnalisée. Ces politiques peuvent fournir divers algorithmes de chiffrement très puissants afin de garantir des communications réseau chiffrées entre les systèmes. Cette règle exige que vous définissiez une politique de sécurité personnalisée pour vos écouteurs SSL. La politique de sécurité par défaut est la suivante : Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256.

ID du contrôle	AWS Règle de configuration	Conseils
2600	elb-custom-security-policy-ssl-check	Pour protéger les données en transit, assurez-vous que vos écouteurs ElasticLoadBalancer SSL classiques utilisent une politique de sécurité personnalisée. Ces politiques peuvent fournir divers algorithmes de chiffrement très puissants afin de garantir des communications réseau chiffrées entre les systèmes. Cette règle exige que vous définissiez une politique de sécurité personnalisée pour vos écouteurs SSL. La politique de sécurité par défaut est la suivante : Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256.
2726	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
3021	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.
3021	kms-cmk- for-each-data-classification (Vérification du processus)	Au moins une clé principale client (CMK) KMS a été définie pour chaque classification de données distincte, et la ou les CMK sont utilisées pour chiffrer toutes les données stockées dans cette classific ation.
3205	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégri té et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
3449	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
3449	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	AWS Règle de configuration	Conseils
3449	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
3451	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
3451	ec2-critical- security-patch-auto-approval (Vérification du processus)	Les référentiels de correctifs pour Windows et/ou Linux ont été configurés dans le Gestionnaire de correctifs, y compris l'approbation automatique des correctifs de sécurité critiques dans les 2 jours suivant leur publication.
3452	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
3452	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateform e disponibles pour l'environ nement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.
3452	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
3453	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
3453	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanées automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
3562	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
3562	cloudfront-associated-with-waf	Ce contrôle vérifie si les CloudFront distributions sont associées aux ACL Web AWS WAF ou AWS WAFv2. Le contrôle échoue si la distribution n'est pas associée à une ACL Web. AWS Le WAF est un pare-feu d'applications Web qui aide à protéger les applications Web et les API contre les attaques. Il vous permet de configurer un ensemble de règles appelé liste de contrôle d'accès web (ACL web) qui autorisent, bloquent ou comptent les requêtes web en fonction des règles et conditions de sécurité web personnalisables que vous définissez. Assurez-vous que votre CloudFront distribution est associée à une ACL Web AWS WAF afin de la protéger contre les attaques malveillantes. Cette règle doit être appliquée dans la région us-east-1.

ID du contrôle	AWS Règle de configuration	Conseils
3562	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3562	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	AWS Règle de configuration	Conseils
3562	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
3562	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
3562	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
3562	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
3562	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
3562	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
3562	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
3562	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
3562	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
3562	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
3562	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
3562	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
3562	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	AWS Règle de configuration	Conseils
3623	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.
3623	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
3623	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
3623	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
3815	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.
3875	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
3875	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS
4333	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
4441	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
4441	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearc h Service.
4441	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
4441	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
4441	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
4441	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
4441	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4445	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
4445	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4829	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.
4829	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibreurs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre application à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	AWS Règle de configuration	Conseils
4829	rds-cluster-multi-az-enabled	La réplication multi-AZ doit être activée sur les clusters Amazon Relational Database Service (Amazon RDS) afin de garantir la disponibilité des données stockées. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
4829	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relational Database Service (Amazon RDS) offre une disponibilité et une durabilité améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibilité. Chaque zone de disponibilité fonctionne sur sa propre infrastructure physiquement distincte et indépendante, et est conçue pour être hautement fiable. En cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	AWS Règle de configuration	Conseils
4838	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
4838	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
4838	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4838	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
4838	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	AWS Règle de configuration	Conseils
4839	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).
4839	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
4839	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
4839	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
4839	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
4839	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	AWS Règle de configuration	Conseils
4839	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
4839	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4839	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
4839	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.
4839	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4839	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
4839	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
4839	sagemaker-endpoint-configur ation-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
4839	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.
4839	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
4839	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
4849	db-instance-backup-enabled	La fonctionnalité de sauvegard e d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	AWS Règle de configuration	Conseils
4849	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.
4849	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	AWS Règle de configuration	Conseils
4849	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
4849	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
4849	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
4849	rds-cluster-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	AWS Règle de configuration	Conseils
4849	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.
4849	rds-instance-deletion-prote ction-enabled	Assurez-vous que la protectio n contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applicati ons.

ID du contrôle	AWS Règle de configuration	Conseils
4849	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.
4849	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	AWS Règle de configuration	Conseils
6843	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
6843	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
6852	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.
6852	federate-with-central-idp (Vérification du processus)	Les identités du personnel nécessitant un accès aux AWS ressources s'authent ifient auprès d'un IdP central AWS fédéré avec le SSO. L'IdP central bloque les utilisateurs du système après 3 tentatives de connexion infructueuses.

ID du contrôle	AWS Règle de configuration	Conseils
6860	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
6860	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
6861	cloudtrail-security-trail-enabled	Cette règle permet de garantir l'utilisation des meilleures pratiques de sécurité AWS recommandées pour AWS CloudTrail, en vérifiant l'activation de plusieurs paramètres. Il s'agit notamment de l'utilisation du chiffrement des journaux, de la validation des journaux et de AWS CloudTrail l'activation dans plusieurs régions.
6953	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
6953	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
7436	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
7436	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
7436	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
7436	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
7437	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
7437	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
7437	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
7437	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
7466	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
7466	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
7466	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.

ID du contrôle	AWS Règle de configuration	Conseils
7466	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
7466	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
7466	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
7466	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
7466	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
7466	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.
7466	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
7466	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
7466	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
7466	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.
7466	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
7466	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.
7466	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	AWS Règle de configuration	Conseils
7466	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.
7496	api-gw-execution-logging-en abled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
7496	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	AWS Règle de configuration	Conseils
7496	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	AWS Règle de configuration	Conseils
7496	cloudfront-accesslogs-enabled	Ce contrôle vérifie si la journalisation des accès au serveur est activée sur les CloudFront distributions. Le contrôle échoue si la journalisation des accès n'est pas activée pour une distribution. CloudFront les journaux d'accès fournisse nt des informations détaillée s sur chaque demande d'utilisateur CloudFront reçue. Chaque journal contient des informations telles que la date et l'heure de réception de la demande, l'adresse IP de l'utilisateur qui a fait la demande, la source de la demande et le numéro de port de la demande formulée par l'utilisateur. Ces journaux sont utiles pour des applicati ons telles que les audits de sécurité et d'accès et les enquêtes judiciaires. Cette règle doit être appliquée dans la région us-east-1.
7496	cloudwatch-log-group-encryp ted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
7496	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.
7496	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	AWS Règle de configuration	Conseils
7496	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for NZISM.

Bonnes pratiques de fonctionnement pour PCI DSS 3.2.1

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) 3.2.1 et les règles de AWS configuration gérées. Chaque AWS Config règle s'applique à une AWS ressource spécifique et concerne un ou plusieurs

contrôles PCI DSS. Un contrôle PCI DSS peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibl es depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplicati on DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaires de cartes, et en particulier refusez tout autre trafic.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePub licAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuck ets les paramètre s (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibl es au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquemen t les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.2.1	Restreignez le trafic entrant et sortant au strict nécessaire pour l'environnement des données de titulaire s de cartes, et en particulier refusez tout autre trafic.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3	Interdisez l'accès public direct entre Internet et tout composant système dans l'environnement des données de titulaires de cartes.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocole s et ports accessibl es publiquement autorisés.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.1	Implémentez une zone DMZ pour limiter le trafic entrant aux seuls composants système qui fournissent des services, protocoles et ports accessibles publiquement autorisés.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.2	Limitez le trafic Internet entrant aux adresses IP comprises dans la zone DMZ.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environ nement de données de titulaires de cartes vers Internet.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environ nement de données de titulaires de cartes vers Internet.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environ nement de données de titulaires de cartes vers Internet.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environ nement de données de titulaires de cartes vers Internet.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppressi on ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environ nement de données de titulaires de cartes vers Internet.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environ nement de données de titulaires de cartes vers Internet.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.4	N'autorisez pas le trafic sortant non autorisé de l'environnement de données de titulaires de cartes vers Internet.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	netfw-policy-rule-group-associated	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic, et vous définissez la gestion du trafic par défaut.
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	netfw-stateless-rule-group-not-empty	Un groupe de règles AWS Network Firewall contient des règles qui définissent la manière dont votre pare-feu traite le trafic dans votre VPC. Un groupe de règles sans état vide, lorsqu'il est présent dans une politique de pare-feu, ne gère pas le trafic.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
1.3.6	Placez les composants système qui stockent les données de titulaires de cartes (comme une base de données) dans une zone réseau interne, séparée de la zone DMZ et des autres réseaux non fiables.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1	Modifiez toujours les valeurs par défaut fournies par le fournisseur et supprimez ou désactivez les comptes par défaut inutiles avant d'installer un système sur le réseau. Cela s'applique à TOUS les mots de passe par défaut, y compris, mais sans s'y limiter, ceux utilisés par les systèmes d'exploitation, les logiciels fournissant des services de sécurité, les comptes d'applications et de systèmes, les terminaux point-of-sale (POS), les applications de paiement, les chaînes communautaires SNMP (Simple Network Management Protocol), etc.).	rds-cluster-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut contribuer à réduire la surface d'attaque de votre ou de vos clusters de base de données Amazon Relational Database Service (Amazon RDS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1	Modifiez toujours les valeurs par défaut fournies par le fournisseur et supprimez ou désactivez les comptes par défaut inutiles avant d'installer un système sur le réseau. Cela s'applique à TOUS les mots de passe par défaut, y compris, mais sans s'y limiter, ceux utilisés par les systèmes d'exploitation, les logiciels fournissant des services de sécurité, les comptes d'applications et de systèmes, les terminaux point-of-sale (POS), les applications de paiement, les chaînes communautaires SNMP (Simple Network Management Protocol), etc.).	rds-instance-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut contribuer à réduire la surface d'attaque de votre ou de vos instances de base de données Amazon Relational Database Service (Amazon RDS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1	Modifiez toujours les valeurs par défaut fournies par le fournisseur et supprimez ou désactivez les comptes par défaut inutiles avant d'installer un système sur le réseau. Cela s'applique à TOUS les mots de passe par défaut, y compris, mais sans s'y limiter, ceux utilisés par les systèmes d'exploitation, les logiciels fournissant des services de sécurité, les comptes d'applications et de systèmes, les terminaux point-of-sale (POS), les applications de paiement, les chaînes communautaires SNMP (Simple Network Management Protocol), etc.).	redshift-default-admin-check	Les noms d'utilisateur par défaut étant connus de tous, leur modification peut réduire la surface d'attaque de votre ou de vos clusters Amazon Redshift.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1	Modifiez toujours les valeurs par défaut fournies par le fournisseur et supprimez ou désactivez les comptes par défaut inutiles avant d'installer un système sur le réseau. Cela s'applique à TOUS les mots de passe par défaut, y compris, mais sans s'y limiter, ceux utilisés par les systèmes d'exploitation, les logiciels fournissant des services de sécurité, les comptes d'applications et de systèmes, les terminaux point-of-sale (POS), les applications de paiement, les chaînes communautaires SNMP (Simple Network Management Protocol), etc.).	redshift-default-db-name-check	Les noms par défaut sont connus du public et doivent être modifiés lors de la configuration. Modifier le nom de la base de données par défaut de votre cluster Amazon Redshift peut contribuer à réduire la surface d'attaque de votre cluster Redshift.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1	Modifiez toujours les valeurs par défaut fournies par le fournisseur et supprimez ou désactivez les comptes par défaut inutiles avant d'installer un système sur le réseau. Cela s'applique à TOUS les mots de passe par défaut, y compris, mais sans s'y limiter, ceux utilisés par les systèmes d'exploitation, les logiciels fournissant des services de sécurité, les comptes d'applications et de systèmes, les terminaux point-of-sale (POS), les applications de paiement, les chaînes communautaires SNMP (Simple Network Management Protocol), etc.).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.1	Modifiez toujours les valeurs par défaut fournies par le fournisseur et supprimez ou désactivez les comptes par défaut inutiles avant d'installer un système sur le réseau. Cela s'applique à TOUS les mots de passe par défaut, y compris, mais sans s'y limiter, ceux utilisés par les systèmes d'exploitation, les logiciels fournissant des services de sécurité, les comptes d'applications et de systèmes, les terminaux point-of-sale (POS), les applications de paiement, les chaînes communautaires SNMP (Simple Network Management Protocol), etc.).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	ec2-instance-multiple-eni-check	Cette règle vérifie si vos instances Amazon Elastic Compute Cloud (Amazon EC2) ont plusieurs ENI. Le fait d'avoir plusieurs ENI peut entraîner la création d'instances à double connexion, c'est-à-dire d'instances ayant plusieurs sous-réseaux. Cela peut ajouter à la complexité de la sécurité du réseau et introduire des chemins et des accès non intentionnels au réseau.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : le Center for Internet Security (CIS), l'Organisation internationale de normalisation (ISO), l'Institut de sécurité des réseaux d' SysAdmin audit (SANS), le National Institute of Standards Technology (NIST).	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	ec2-security-group-attached-to-eni-periodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveiller les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : le Center for Internet Security (CIS), l'Organisation internationale de normalisation (ISO), l'Institut de sécurité des réseaux d' SysAdmin audit (SANS), le National Institute of Standards Technology (NIST).	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2	Développez des normes de configuration pour tous les composants système. Assurez-vous que ces normes répondent à toutes les vulnérabilités de sécurité connues et sont conformes aux normes relatives à la sécurisation renforcée des systèmes acceptées par le secteur. Les sources des normes de renforcement des systèmes acceptées par l'industrie peuvent inclure, sans toutefois s'y limiter : • le Center for Internet Security (CIS) • l'Organisation internationale de normalisation (ISO) • l'Institut de sécurité des réseaux SysAdmin d'audit (SANS) • le National Institute of Standards Technology (NIST).	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.2	Activez uniquement les services, protocoles, démons, etc. nécessaires au fonctionnement du système.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.2.3	Mettez en œuvre des fonctionnalités de sécurité supplémentaires pour tous les services, protocoles ou démons requis considérés comme non sécurisés.	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.3	Chiffrez tous les accès administratifs hors console à l'aide d'un chiffrement fort.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
2.3	Chiffrez tous les accès administratifs hors console à l'aide d'un chiffrement fort.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.3	Chiffrez tous les accès administratifs hors console à l'aide d'un chiffrement fort.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
2.3	Chiffrez tous les accès administratifs hors console à l'aide d'un chiffrement fort.	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2.3	Chiffrez tous les accès administratifs hors console à l'aide d'un chiffrement fort.	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
2,4	Tenez à jour un inventaire des composants système qui sont concernés par la norme PCI DSS.	ec2-security-group -attached-to-eni-p eriodic	Cette règle garantit que les groupes de sécurité sont associés à une instance Amazon Elastic Compute Cloud (Amazon EC2) ou à une ENI. Cette règle permet de surveille r les groupes de sécurité non utilisés dans l'inventaire et de gérer votre environne ment.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2,4	Tenez à jour un inventaire des composants système qui sont concernés par la norme PCI DSS.	eip-attached	Cette règle garantit que les adresses IP Elastic (EIP) allouées à un réseau Amazon Virtual Private Cloud (Amazon VPC) sont attachées aux instances Amazon Elastic Compute Cloud (Amazon EC2) ou aux interfaces réseaux Elastic (ENI) en cours d'utilisation. Cette règle permet de surveiller les EIP non utilisées dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2,4	Tenez à jour un inventaire des composants système qui sont concernés par la norme PCI DSS.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
2,4	Tenez à jour un inventaire des composants système qui sont concernés par la norme PCI DSS.	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées . La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1	Limitez le stockage des données de titulaires de cartes au minimum en mettant en œuvre des politiques et des procédure s de conservat ion et d'élimina tion des données qui comprenne nt au moins les éléments suivants pour l'ensemble du stockage des données de titulaire s de cartes (CHD) : • Limitation de la quantité de stockage et de la durée de conservation des données à ce qui est nécessaire pour répondre aux exigences légales, réglementaires et/ ou commerciales • Exigences de conservation spécifiqu es pour les données de titulaires de cartes • Procédure de suppression sécurisée	s3-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des données lorsqu'elles ne sont plus nécessaires • Une procédure trimestrielle d'identification et de suppression sécurisée des données de titulaires de cartes stockées qui dépassent les durées de conservation définies.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1	Limitez le stockage des données de titulaires de cartes au minimum en mettant en œuvre des politiques et des procédures de conservation et d'élimination des données qui comprennent au moins les éléments suivants pour l'ensemble du stockage des données de titulaires de cartes (CHD) : • Limitation de la quantité de stockage et de la durée de conservation des données à ce qui est nécessaire pour répondre aux exigences légales, réglementaires et/ou commerciales • Exigences de conservation spécifiques pour les données de titulaires de cartes • Procédure de suppression sécurisée	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des données lorsqu'elles ne sont plus nécessaires • Une procédure trimestrielle d'identification et de suppression sécurisée des données de titulaires de cartes stockées qui dépassent les durées de conservation définies.		nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1	Limitez le stockage des données de titulaires de cartes au minimum en mettant en œuvre des politiques et des procédures de conservation et d'élimination des données qui comprennent au moins les éléments suivants pour l'ensemble du stockage des données de titulaires de cartes (CHD) : • Limitation de la quantité de stockage et de la durée de conservation des données à ce qui est nécessaire pour répondre aux exigences légales, réglementaires et/ou commerciales • Exigences de conservation spécifiques pour les données de titulaires de cartes • Procédure de suppression sécurisée	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des données lorsqu'elles ne sont plus nécessaires • Une procédure trimestrielle d'identification et de suppression sécurisée des données de titulaires de cartes stockées qui dépassent les durées de conservation définies.		exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1	Limitez le stockage des données de titulaires de cartes au minimum en mettant en œuvre des politiques et des procédure s de conservat ion et d'élimina tion des données qui comprenne nt au moins les éléments suivants pour l'ensemble du stockage des données de titulaire s de cartes (CHD) : • Limitation de la quantité de stockage et de la durée de conservation des données à ce qui est nécessaire pour répondre aux exigences légales, réglementaires et/ ou commerciales • Exigences de conservation spécifiqu es pour les données de titulaires de cartes • Procédure de suppression sécurisée	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	des données lorsqu'elles ne sont plus nécessaires • Une procédure trimestrielle d'identification et de suppression sécurisée des données de titulaires de cartes stockées qui dépassent les durées de conservation définies.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirectionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissages (les remplissages doivent être stockés de manière sécurisée) • Chiffrement puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-v ous que le chiffreme nt est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-v ous que le chiffreme nt est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirectionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissages (les remplissages doivent être stockés de manière sécurisée) • Chiffrement puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relationa l Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirectionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissages (les remplissages doivent être stockés de manière sécurisée) • Chiffrement puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirectionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissages (les remplissages doivent être stockés de manière sécurisée) • Chiffrement puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirectionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncature (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissages (les remplissages doivent être stockés de manière sécurisée) • Chiffrement puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	sagemaker-endpoint -configuration-kms- key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	sagemaker-notebook -instance-kms-key- configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-note s, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.4	Rendez le numéro PAN illisible partout où il est stocké (y compris sur les supports numériques portables , les supports de sauvegarde et dans les journaux) à l'aide de l'une des approches suivantes : • Hachage unidirect ionnel basé sur un chiffrement fort (le hachage doit porter sur tout le numéro PAN) • Troncatur e (le hachage ne peut pas être utilisé pour remplacer le segment tronqué du numéro PAN) • Jetons d'index et remplissa ges (les remplissa ges doivent être stockés de manière sécurisée) • Chiffreme nt puissant associé aux procédures de gestion des clés associés. Remarque : il est relativement facile pour une	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	personne malveillante de reconstituer les données originales du numéro PAN si elle a accès à la fois à la version tronquée et à la version hachée d'un numéro PAN. Lorsque des versions hachées et tronquées du même numéro PAN sont présentes dans l'environnement d'une entité, des contrôles supplémentaires doivent être mis en place pour s'assurer que les versions hachées et tronquées ne peuvent pas être mises en corrélation pour reconstituer le numéro PAN d'origine.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2	Limitez l'accès aux clés de chiffrement au plus petit nombre possible de dépositaires.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.2	Limitez l'accès aux clés de chiffrement au plus petit nombre possible de dépositaires.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.3	Stockez à tout moment les clés secrètes et privées utilisées pour crypter/déchiffrer les données des titulaires de carte sous l'une (ou plusieurs) des formes suivantes : • Chiffrées à l'aide d'une clé au moins aussi puissante que la clé de cryptage des données et stockée séparément de la clé de cryptage des données • Au sein d'un dispositif cryptographique sécurisé (tel qu'un module de sécurité matériel (hôte) (HSM) ou un point-of-interaction appareil approuvé par le PTS) • Au moins deux longueur des composants clés ou des partages de clés, conformément à une méthode acceptée par l'industrie Remarque : Il n'est pas nécessaire que les clés publiques	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	soient stockées dans l'un des ces formulaires.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.3	Stockez à tout moment les clés secrètes et privées utilisées pour crypter/déchiffrer les données des titulaires de carte sous l'une (ou plusieurs) des formes suivantes : • Chiffrées à l'aide d'une clé au moins aussi puissante que la clé de cryptage des données et stockée séparément de la clé de cryptage des données • Au sein d'un dispositif cryptographique sécurisé (tel qu'un module de sécurité matériel (hôte) (HSM) ou un point-of-interaction appareil approuvé par le PTS) • Au moins deux longueur des composants clés ou des partages de clés, conformément à une méthode acceptée par l'industrie Remarque : Il n'est pas nécessaire que les clés publiques	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	soient stockées dans l'un des ces formulaires.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.5.3	Stockez à tout moment les clés secrètes et privées utilisées pour crypter/déchiffrer les données des titulaires de carte sous l'une (ou plusieurs) des formes suivantes : • Chiffrées à l'aide d'une clé au moins aussi puissante que la clé de cryptage des données et stockée séparément de la clé de cryptage des données • Au sein d'un dispositif cryptographique sécurisé (tel qu'un module de sécurité matériel (hôte) (HSM) ou un point-of-interaction appareil approuvé par le PTS) • Au moins deux longueur des composants clés ou des partages de clés, conformément à une méthode acceptée par l'industrie Remarque : Il n'est pas nécessaire que les clés publiques	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	soient stockées dans l'un des ces formulaires.		
3.6.4	Changements de clés de chiffrement pour les clés qui ont atteint la fin de leur période de chiffrement (par exemple, après une période de temps définie et/ou après qu'une certaine quantité de texte chiffré a été produite par une clé donnée), comme défini par le fournisseur de l'application ou le propriétaire de la clé associé, et selon les bonnes pratiques et les directives de l'industrie (par exemple, la publication spéciale 800-57 du NIST).	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.5	Retrait ou remplacement (par exemple, archivage, destruction et/ou révocation) des clés si cela est jugé nécessaire lorsque l'intégrité de la clé a été affaiblie (par exemple, départ d'un employé ayant connaissance d'un composant de clé en clair) ou que l'on soupçonne que les clés ont été compromises. Note : Si des clés de chiffrement retirées ou remplacées doivent être conservées, ces clés doivent être archivées de manière sécurisée (par exemple, à l'aide d'une clé de chiffrement). Les clés de chiffrement archivées ne doivent être utilisées qu'à des fins de déchiffrement/vérification.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.6.7	Prévention de la substitution non autorisée de clés de chiffrement.	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certificats de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configurations sécurisées. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprennent, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulaires, par exemple, le système mondial	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certifica ts de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configura tions sécurisée s. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprenne nt, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulair es, par exemple, le système mondial	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certifica ts de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configura tions sécurisée s. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprenne nt, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulair es, par exemple, le système mondial	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certifica ts de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configura tions sécurisée s. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprenne nt, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulair es, par exemple, le système mondial	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certifica ts de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configura tions sécurisée s. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprenne nt, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulair es, par exemple, le système mondial	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certifica ts de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configura tions sécurisée s. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprenne nt, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulair es, par exemple, le système mondial	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-v ous que le chiffreme nt est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certificats de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configurations sécurisées. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprennent, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulaires, par exemple, le système mondial	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certifica ts de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configura tions sécurisée s. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprenne nt, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulair es, par exemple, le système mondial	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearc h Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certifica ts de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configura tions sécurisée s. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprenne nt, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulair es, par exemple, le système mondial	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.1	Utilisez un chiffrement et des protocoles de sécurité robustes pour protéger les données sensibles de titulaires de cartes lors de leur transmission sur des réseaux ouverts et publics, notamment les suivants : • Seuls les clés et les certificats de confiance sont acceptés. • Le protocole utilisé ne prend en charge que des versions ou des configurations sécurisées. • Le niveau de chiffrement est adapté à la méthode de chiffrement utilisée. Les exemples de réseaux ouverts et publics comprennent, sans toutefois s'y limiter : • Internet • Les technologies sans fil, notamment 802.11 et Bluetooth • Les technologies cellulaires, par exemple, le système mondial	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	de communications mobiles (GSM), l'accès multiple par répartition en code (CDMA) • Le service général de radiocommunication par paquets (GPRS) • Les communications par satellite		
6.2	Assurez-vous que tous les composants système et logiciels sont protégés contre les vulnérabilités connues en installant les correctifs de sécurité fournis par le fournisseur. Installez les correctifs de sécurité critiques dans le mois qui suit leur publication. Remarque : Les correctifs de sécurité critiques doivent être identifiés conformément à la procédure de classement des risques définie dans l'exigence 6.1.	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.2	Assurez-vous que tous les composants système et logiciels sont protégés contre les vulnérabilités connues en installant les correctifs de sécurité fournis par le fournisseur. Installez les correctifs de sécurité critiques dans le mois qui suit leur publication. Remarque : Les correctifs de sécurité critiques doivent être identifiés conformément à la procédure de classement des risques définie dans l'exigence 6.1.	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.2	Assurez-vous que tous les composants système et logiciels sont protégés contre les vulnérabilités connues en installant les correctifs de sécurité fournis par le fournisseur. Installez les correctifs de sécurité critiques dans le mois qui suit leur publication. Remarque : Les correctifs de sécurité critiques doivent être identifiés conformément à la procédure de classement des risques définie dans l'exigence 6.1.	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.2	Assurez-vous que tous les composants système et logiciels sont protégés contre les vulnérabilités connues en installant les correctifs de sécurité fournis par le fournisseur. Installez les correctifs de sécurité critiques dans le mois qui suit leur publication. Remarque : Les correctifs de sécurité critiques doivent être identifiés conformément à la procédure de classement des risques définie dans l'exigence 6.1.	ecs-fargate-latest-platform-version	Les mises à jour de sécurité et les correctifs sont déployés automatiquement pour vos tâches AWS Fargate. Si un problème de sécurité affectant une version de la plateforme AWS Fargate est détecté AWS , corrige la version de la plate-forme. Pour faciliter la gestion des correctifs de vos tâches Amazon Elastic Container Service (ECS) exécutant AWS Fargate, mettez à jour les tâches autonomes de vos services afin d'utiliser la version la plus récente de la plateforme.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.2	Assurez-vous que tous les composants système et logiciels sont protégés contre les vulnérabilités connues en installant les correctifs de sécurité fournis par le fournisseur. Installez les correctifs de sécurité critiques dans le mois qui suit leur publication. Remarque : Les correctifs de sécurité critiques doivent être identifiés conformément à la procédure de classement des risques définie dans l'exigence 6.1.	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.2	Assurez-vous que tous les composants système et logiciels sont protégés contre les vulnérabilités connues en installant les correctifs de sécurité fournis par le fournisseur. Installez les correctifs de sécurité critiques dans le mois qui suit leur publication. Remarque : Les correctifs de sécurité critiques doivent être identifiés conformément à la procédure de classement des risques définie dans l'exigence 6.1.	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3.2	Passez en revue le code personnalisé avant sa diffusion à la production ou aux clients afin d'identifier toute vulnérabilité de codage potentielle (à l'aide de procédure s manuelles ou automatisées), de manière à inclure au moins les éléments suivants : • Les modifications du code sont examinées par des personnes autres que l'auteur du code d'origine et par des personnes connaissa nt les techniques d'examen du code et les pratiques de codage sécurisé. • Les examens du code garantissent que le code est développé conformém ent aux directives de codage sécurisé • Les corrections appropriées sont mises en œuvre avant la publication. • Les	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur . L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégri té et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	résultats de l'examen du code sont passés en revue et approuvés par la direction avant leur publication. (Suite à la page suivante)		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,6	Pour les applications web accessibles au public, répondez en permanence aux nouvelles menaces et vulnérabilités et veillez à ce que ces applications soient protégées contre les attaques connues en appliquant l'une des méthodes suivantes : • Examen des applications web destinées au public à l'aide d'outils ou de méthodes d'évaluation manuelle ou automatisée de la sécurité des vulnérabilités des applications, au moins une fois par an et après toute modification. Remarque : Cette évaluation n'est pas identique à l'analyse des vulnérabilités effectuée pour l'exigence 11.2. • Installation d'une solution technique automatisée qui	alb-desync-mode-check	Pour faciliter la protection des applications contre les vulnérabilités HTTP Desync, assurez-vous que le mode d'atténuation HTTP Desync est activé sur vos équilibreurs de charge d'application. Les problèmes de désynchronisation HTTP peuvent entraîner la dissimulation de requêtes et rendre vos applications vulnérables à l'empoisonnement de la file d'attente des requêtes ou du cache. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. Le mode défensif est le mode par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	détecte et empêche les attaques basées sur le web (par exemple, un pare-feu d'application web) devant les applications web orientées vers le public, afin de contrôler en permanence l'ensemble du trafic.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,6	Pour les applications web accessibles au public, répondez en permanence aux nouvelles menaces et vulnérabilités et veillez à ce que ces applications soient protégées contre les attaques connues en appliquant l'une des méthodes suivantes : • Examen des applications web destinées au public à l'aide d'outils ou de méthodes d'évaluation manuelle ou automatisée de la sécurité des vulnérabilités des applications, au moins une fois par an et après toute modification. Remarque : Cette évaluation n'est pas identique à l'analyse des vulnérabilités effectuée pour l'exigence 11.2. • Installation d'une solution technique automatisée qui	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	détecte et empêche les attaques basées sur le web (par exemple, un pare-feu d'application web) devant les applications web orientées vers le public, afin de contrôler en permanence l'ensemble du trafic.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,6	Pour les applications web accessibles au public, répondez en permanence aux nouvelles menaces et vulnérabilités et veillez à ce que ces applications soient protégées contre les attaques connues en appliquant l'une des méthodes suivantes : • Examen des applications web destinées au public à l'aide d'outils ou de méthodes d'évaluation manuelle ou automatisée de la sécurité des vulnérabilités des applications, au moins une fois par an et après toute modification. Remarque : Cette évaluation n'est pas identique à l'analyse des vulnérabilités effectuée pour l'exigence 11.2. • Installation d'une solution technique automatisée qui	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	détecte et empêche les attaques basées sur le web (par exemple, un pare-feu d'application web) devant les applications web orientées vers le public, afin de contrôler en permanence l'ensemble du trafic.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,6	Pour les applications web accessibles au public, répondez en permanence aux nouvelles menaces et vulnérabilités et veillez à ce que ces applications soient protégées contre les attaques connues en appliquant l'une des méthodes suivantes : • Examen des applications web destinées au public à l'aide d'outils ou de méthodes d'évaluation manuelle ou automatisée de la sécurité des vulnérabilités des applications, au moins une fois par an et après toute modification. Remarque : Cette évaluation n'est pas identique à l'analyse des vulnérabilités effectuée pour l'exigence 11.2. • Installation d'une solution technique automatisée qui	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	détecte et empêche les attaques basées sur le web (par exemple, un pare-feu d'application web) devant les applications web orientées vers le public, afin de contrôler en permanence l'ensemble du trafic.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,6	Pour les applications web accessibles au public, répondez en permanence aux nouvelles menaces et vulnérabilités et veillez à ce que ces applications soient protégées contre les attaques connues en appliquant l'une des méthodes suivantes : • Examen des applications web destinées au public à l'aide d'outils ou de méthodes d'évaluation manuelle ou automatisée de la sécurité des vulnérabilités des applications, au moins une fois par an et après toute modification. Remarque : Cette évaluation n'est pas identique à l'analyse des vulnérabilités effectuée pour l'exigence 11.2. • Installation d'une solution technique automatisée qui	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	détecte et empêche les attaques basées sur le web (par exemple, un pare-feu d'application web) devant les applications web orientées vers le public, afin de contrôler en permanence l'ensemble du trafic.		

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6,6	Pour les applications web accessibles au public, répondez en permanence aux nouvelles menaces et vulnérabilités et veillez à ce que ces applications soient protégées contre les attaques connues en appliquant l'une des méthodes suivantes : • Examen des applications web destinées au public à l'aide d'outils ou de méthodes d'évaluation manuelle ou automatisée de la sécurité des vulnérabilités des applications, au moins une fois par an et après toute modification. Remarque : Cette évaluation n'est pas identique à l'analyse des vulnérabilités effectuée pour l'exigence 11.2. • Installation d'une solution technique automatisée qui	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL Web est vide, le trafic Web n'est pas détecté ni traité par le WAF.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
	détecte et empêche les attaques basées sur le web (par exemple, un pare-feu d'application web) devant les applications web orientées vers le public, afin de contrôler en permanence l'ensemble du trafic.		
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composants système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	s3-bucket-acl-proh ibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanisme s de contrôle d'accès existants pour les compartiments Amazon S3 antérieur s à AWS Identity and Access Management (IAM). Au lieu d'utilise r des listes ACL, il est recommandé d'utiliser des politique s IAM ou des politique s de compartim ent S3 pour gérer plus facilement l'accès à vos compartim ents S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	ecs-containers-rea donly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instanc e de conteneur ne peut être modifié que s'il dispose d'autoris ations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	efs-access-point-e nforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répe rtoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	efs-access-point-e nforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisa teur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composants système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composants système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composants système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.1	Définissez les besoins d'accès pour chaque rôle, notamment : • Les composant s système et les ressources de données auxquels chaque rôle doit accéder dans le cadre de sa fonction • Le niveau de privilège requis (par exemple, utilisateur, administrateur, etc.) pour accéder aux ressources.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearc h Service. Le contrôle d'accès précis fournit des mécanisme s d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authent ification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégi és aux privilèges minimaux nécessair es à l'exercice de leurs responsabilités professionnelles.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégiés aux privilèges minimaux nécessaires à l'exercice de leurs responsabilités professionnelles.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégi és aux privilèges minimaux nécessair es à l'exercice de leurs responsabilités professionnelles.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégiés aux privilèges minimaux nécessaires à l'exercice de leurs responsabilités professionnelles.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégiés aux privilèges minimaux nécessaires à l'exercice de leurs responsabilités professionnelles.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégiés aux privilèges minimaux nécessaires à l'exercice de leurs responsabilités professionnelles.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégi és aux privilèges minimaux nécessair es à l'exercice de leurs responsabilités professionnelles.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégiés aux privilèges minimaux nécessaires à l'exercice de leurs responsabilités professionnelles.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.1.2	Limitez l'accès aux ID d'utilisateurs privilégiés aux privilèges minimaux nécessaires à l'exercice de leurs responsabilités professionnelles.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	ecs-containers-rea donly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instanc e de conteneur ne peut être modifié que s'il dispose d'autoris ations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	efs-access-point-e nforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répe rtoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	efs-access-point-e nforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisa teur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composants système qui limite l'accès en fonction du besoin d'informations de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-policy-no-stat ements-with-full-a ccess	Assurez-vous que les actions IAM sont limitées aux seules actions nécessair es. Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composants système qui limite l'accès en fonction du besoin d'informations de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.1	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisa teur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce système de contrôle d'accès doit comprendre les éléments suivants : Couverture de tous les composants système	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearc h Service. Le contrôle d'accès précis fournit des mécanisme s d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authent ification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	ecs-containers-non privileged	Pour faciliter la mise en œuvre du principe du moindre privilège, les définitions de tâches Amazon Elastic Container Service (Amazon ECS) ne doivent pas comporter de privilèges élevés. Quand ce paramètre a la valeur true, le conteneur dispose de droits élevés sur l'instance de conteneur hôte (similaire à l'utilisateur root).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	ecs-containers-rea donly-access	L'activation de l'accès en lecture seule aux conteneurs Amazon Elastic Container Service (ECS) permet de respecter le principe du moindre privilège. Cette option peut réduire les vecteurs d'attaque , car le système de fichiers de l'instanc e de conteneur ne peut être modifié que s'il dispose d'autoris ations explicites de lecture et d'écriture.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	efs-access-point-e nforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répe rtoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	efs-access-point-e nforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisa teur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Managemen t) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisa tion, la gestion des versions, la restaurat ion, ainsi que la délégation de la gestion des autorisat ions. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéA WS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			refléter les politiques de votre organisation.
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-policy-no-stat ements-with-admin-access	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparatio n des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilège s que nécessaire pour effectuer une tâche peut enfreindr e le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composants système qui limite l'accès en fonction du besoin d'informations de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendre les éléments suivants : Attribution de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composants système qui limite l'accès en fonction du besoin d'informations de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendre les éléments suivants : Attribution de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et les autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.2	Établissez un système de contrôle d'accès pour les composant s système qui limite l'accès en fonction du besoin d'informa tions de l'utilisateur et qui est défini sur « tout refuser » sauf autorisation expresse. Ce ou ces systèmes de contrôle des accès doivent comprendr e les éléments suivants : Attributi on de privilèges aux personnes en fonction de leur classification professionnelle et de leur fonction.	opensearch-access-control-enabled	Assurez-vous que le contrôle d'accès détaillé est activé sur vos domaines Amazon OpenSearc h Service. Le contrôle d'accès précis fournit des mécanisme s d'autorisation améliorés pour obtenir un accès moins privilégié aux domaines Amazon Service. OpenSearch Il permet un contrôle d'accès au domaine basé sur les rôles, ainsi que la sécurité au niveau des index, des documents et des champs, la prise en charge des tableaux de bord de OpenSearch service, la mutualisation des tableaux de bord des services et l'authent ification HTTP de base pour Service et Kibana. OpenSearch

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
7.2.3	Paramètre « Tout refuser » par défaut.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1.1	Attribuez à tous les utilisateurs un ID unique avant de leur permettre d'accéder aux composants système ou aux données de titulaires de cartes.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1.4	Supprimez/désactivez les comptes utilisateurs inactifs dans un délai de 90 jours.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	codebuild-project-environment-privileged-check	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous que le mode privilégié n'est pas activé dans votre environnement de CodeBuild projet Amazon. Ce paramètre doit être désactivé pour empêcher tout accès imprévu aux API Docker ainsi qu'au matériel sous-jacent du conteneur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	ecs-no-environment-secrets	La pratique exemplaire en matière de sécurité consiste à transmettre les informations sensibles aux conteneurs sous la forme de variables d'environnement. Vous pouvez injecter des données en toute sécurité dans vos conteneurs Amazon Elastic Container Service (ECS) en référençant les valeurs stockées dans AWS le Parameter Store ou dans le AWS Secrets Manager dans la définition de conteneur d'une définition de tâche Amazon ECS. Vous pouvez ensuite exposer vos informations sensibles en tant que variables d'environnement ou dans la configuration de journal d'un conteneur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffrement au repos pour protéger ces données.
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.1	À l'aide d'un chiffrement fort, rendez illisibles toutes les informations d'authentification (comme les mots de passe/expressions) pendant la transmission et le stockage sur tous les composants système.	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l'AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.3	Les mots de passe/phrases secrètes doivent satisfaire les critères suivants : • Avoir une longueur minimale d'au moins sept caractères. • Contenir à la fois des caractères numériques et alphabétiques. À défaut, les mots de passe/phrases secrètes doivent être d'une complexité et d'une force au moins équivalentes aux paramètres spécifiés ci-dessus.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (PCI DSS par défaut : false), RequireLowercaseCharacters (PCI DSS par défaut : true), (PCI DSS par défaut : false), RequireSymbols (PCI DSS par défaut : true), RequireNumbers (PCI DSS par défaut : 7), MinimumPa

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sswordLength (PCI DSS par défaut : 4) et PasswordReusePreve ntion MaxPasswo rdAge (PCI DSS par défaut : 90) pour votre politique de mot de passe IAM. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.4	Modifiez les mots de passe/phrases de passe des utilisateurs au moins tous les 90 jours.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.4	Modifiez les mots de passe/phrases de passe des utilisateurs au moins tous les 90 jours.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (PCI DSS par défaut : false), RequireLowercaseCharacters (PCI DSS par défaut : true), (PCI DSS par défaut : false), RequireSymbols (PCI DSS par défaut : true), RequireNumbers (PCI DSS par défaut : 7), MinimumPa

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sswordLength (PCI DSS par défaut : 4) et PasswordReusePreve ntion MaxPasswo rdAge (PCI DSS par défaut : 90) pour votre politique de mot de passe IAM. Les valeurs réelles doivent refléter les politiques de votre organisation.
8.2.4	Modifiez les mots de passe/phrases de passe des utilisateurs au moins tous les 90 jours.	secretsmanager-rot ation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiel lement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.2.5	Ne permettez pas à une personne de soumettre un nouveau mot de passe/une nouvelle phrase secrète qui soit identique aux quatre derniers mots de passe/phrases secrètes qu'elle a utilisés.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (PCI DSS par défaut : false), RequireLowercaseCharacters (PCI DSS par défaut : true), (PCI DSS par défaut : false), RequireSymbols (PCI DSS par défaut : true), RequireNumbers (PCI DSS par défaut : 7), MinimumPa

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sswordLength (PCI DSS par défaut : 4) et PasswordReusePreve ntion MaxPasswo rdAge (PCI DSS par défaut : 90) pour votre politique de mot de passe IAM. Les valeurs réelles doivent refléter les politiques de votre organisation.
8.3.1	Incorporez l'authent ification multifacteur pour tous les accès autres que via la console dans le CDE pour le personnel disposant d'un accès administrateur.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressource s dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémen taire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3.1	Incorporez l'authentification multifacteur pour tous les accès autres que via la console dans le CDE pour le personnel disposant d'un accès administrateur.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3.1	Incorporez l'authentification multifacteur pour tous les accès autres que via la console dans le CDE pour le personnel disposant d'un accès administrateur.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3.1	Incorporez l'authentification multifacteur pour tous les accès autres que via la console dans le CDE pour le personnel disposant d'un accès administrateur.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3.2	Incorporez l'authentification multifacteur pour tous les accès réseau distants (utilisateur et administrateur, y compris l'accès tiers pour le support ou la maintenance) provenant de l'extérieur du réseau de l'entité.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3.2	Incorporez l'authentification multifacteur pour tous les accès réseau distants (utilisateur et administrateur, y compris l'accès tiers pour le support ou la maintenance) provenant de l'extérieur du réseau de l'entité.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. L'authentification MFA ajoute une couche de sécurité supplémentaire, en plus d'un nom d'utilisateur et d'un mot de passe. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3.2	Incorporez l'authentification multifacteur pour tous les accès réseau distants (utilisateur et administrateur, y compris l'accès tiers pour le support ou la maintenance) provenant de l'extérieur du réseau de l'entité.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.3.2	Incorporez l'authentification multifacteur pour tous les accès réseau distants (utilisateur et administrateur, y compris l'accès tiers pour le support ou la maintenance) provenant de l'extérieur du réseau de l'entité.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. L'authentification MFA ajoute une couche de sécurité supplémentaire pour un nom d'utilisateur et un mot de passe. En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.1	Mettez en œuvre des journaux de piste d'audit pour relier tous les accès aux composants système à chaque utilisateur.	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événement s suivants : Tous les accès d'utilisa teurs individuels aux données de titulaires de cartes	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.2.1	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événement s suivants : Tous les accès d'utilisa teurs individuels aux données de titulaires de cartes	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.1	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tous les accès d'utilisateurs individuels aux données de titulaires de cartes	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.2	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Toutes les actions effectuées par une personne disposant de privilèges racine ou administrateur	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.2.3	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événement s suivants : Accès à toutes les pistes d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.3	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Accès à toutes les pistes d'audit	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tentatives d'accès logique non valide	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Tentatives d'accès logique non valide	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.2.4	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Tentatives d'accès logique non valide	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Tentatives d'accès logique non valide	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tentatives d'accès logique non valide	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
10.2.4	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tentatives d'accès logique non valide	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Tentatives d'accès logique non valide	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tentatives d'accès logique non valide	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Tentatives d'accès logique non valide	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Tentatives d'accès logique non valide	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.4	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Tentatives d'accès logique non valide	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.5	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Utilisation et modification des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation des privilèges, ainsi que tous les ajouts, suppressions ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.2.5	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événement s suivants : Utilisati on et modification des mécanismes d'identification et d'authentification , y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévati on des privilèges, ainsi que tous les ajouts, suppressi ons ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.5	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Utilisation et modification des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation des privilèges, ainsi que tous les ajouts, suppressions ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.5	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événement s suivants : Utilisati on et modification des mécanismes d'identification et d'authentification , y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévati on des privilèges, ainsi que tous les ajouts, suppressi ons ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.5	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Utilisation et modification des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation des privilèges, ainsi que tous les ajouts, suppressions ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.5	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Utilisation et modification des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation des privilèges, ainsi que tous les ajouts, suppressions ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.5	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Utilisation et modification des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation des privilèges, ainsi que tous les ajouts, suppressions ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.5	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Utilisation et modification des mécanismes d'identification et d'authentification, y compris, mais sans s'y limiter, la création de nouveaux comptes et l'élévation des privilèges, ainsi que tous les ajouts, suppressions ou modifications effectués sur des comptes dotés de privilèges racine ou administrateur	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.6	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Initialisation, arrêt ou pause des journaux d'audit	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.2.6	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événement s suivants : Initialis ation, arrêt ou pause des journaux d'audit	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.6	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Initialisation, arrêt ou pause des journaux d'audit	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
10.2.7	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Création et suppression d'objets au niveau du système	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.7	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Création et suppression d'objets au niveau du système	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisate urs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrai l fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REG ION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.2.7	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Création et suppression d'objets au niveau du système	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.7	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Création et suppression d'objets au niveau du système	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnosti c des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.7	Implémentez des journaux de piste d'audit automatiques pour tous les composants système afin de reconstruire les événements suivants : Création et suppression d'objets au niveau du système	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.7	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Création et suppression d'objets au niveau du système	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatc h Logs à des fins de conservation et de réponse. OpenSearc h Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.2.7	Implémentez des journaux de piste d'audit automatiq ues pour tous les composants système afin de reconstru ire les événements suivants : Création et suppression d'objets au niveau du système	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environne ment, assurez-vous que la journalisation Amazon Relationa l Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexion s, des déconnexions, des requêtes ou des tables interrogées.
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identific ation de l'utilisateur	api-gw-execution-l ogging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informati ons offrent une visibilit é sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécurité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.3.1	Enregistrez au moins les entrées de journaux de piste d'audit suivantes pour tous les composants système pour chaque événement : Identification de l'utilisateur	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5	Sécurisez les pistes d'audit afin qu'elles ne puissent pas être modifiées.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
10.5	Sécurisez les pistes d'audit afin qu'elles ne puissent pas être modifiées.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartim ents Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5	Sécurisez les pistes d'audit afin qu'elles ne puissent pas être modifiées.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
10.5.2	Protégez les fichiers journaux de piste d'audit contre les modifications non autorisées.	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5.2	Protégez les fichiers journaux de piste d'audit contre les modifications non autorisées.	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
10.5.2	Protégez les fichiers journaux de piste d'audit contre les modifications non autorisées.	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5.3	Sauvegardez rapidement les fichiers de journaux de piste d'audit sur un serveur de journaux centralisé ou un support difficile à modifier.	s3-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5.3	Sauvegardez rapidement les fichiers de journaux de piste d'audit sur un serveur de journaux centralisé ou un support difficile à modifier.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
10.5.3	Sauvegardez rapidement les fichiers de journaux de piste d'audit sur un serveur de journaux centralisé ou un support difficile à modifier.	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5.3	Sauvegardez rapidement les fichiers de journaux de piste d'audit sur un serveur de journaux centralisé ou un support difficile à modifier.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5.5	Utilisez un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications sur les journaux pour s'assurer que les données de journal existantes ne peuvent pas être modifiées sans générer d'alertes (bien que l'ajout de nouvelles données ne doive pas provoquer d'alerte).	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.5.5	Utilisez un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications sur les journaux pour s'assurer que les données de journal existantes ne peuvent pas être modifiées sans générer d'alertes (bien que l'ajout de nouvelles données ne doive pas provoquer d'alerte).	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartim ent Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicati ve.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.7	Conservez l'histori que des pistes d'audit pendant au moins un an, avec un minimum de trois mois immédiate ment disponibles pour analyse (par exemple, en ligne, archivé ou restaurable à partir d'une sauvegarde).	s3-lifecycle-policy-check	Assurez-vous que les politiques de cycle de vie d'Amazon S3 sont configurées pour vous aider à définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transfére r les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'une certaine période).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
10.7	Conservez l'histori que des pistes d'audit pendant au moins un an, avec un minimum de trois mois immédiate ment disponibles pour analyse (par exemple, en ligne, archivé ou restaurable à partir d'une sauvegarde).	backup-plan-min-fr equency-and-min-re tention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegard e est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e. Cette règle vous permet de définir les paramètres requiredFrequencyV alue (Config par défaut : 1), requiredR etentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
11.2.3	Effectuez des analyses internes et externes et, le cas échéant, de nouvelles analyses après toute modification importante. Les analyses doivent être effectuées par du personnel qualifié.	ecr-private-image-scanning-enabled	La numérisation d'images Amazon Elastic Container Repository (ECR) permet d'identifier les vulnérabilités logicielles dans vos images de conteneur. L'activation de la numérisation d'images dans les référentiels ECR ajoute une couche de vérification de l'intégrité et de la sécurité des images stockées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Utilisez des techniques de détection et/ou de prévention des intrusions pour détecter et/ou empêcher les intrusions dans le réseau. Surveillez l'ensemble du trafic au périmètre de l'environnement des données de titulaires de cartes ainsi qu'aux points critiques de l'environnement des données de titulaires de cartes, et alertez le personnel en cas de suspicion de compromission. Maintenez à jour tous les moteurs, bases de référence et signatures de détection et de prévention des intrusions.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.4	Utilisez des techniques de détection et/ou de prévention des intrusions pour détecter et/ou empêcher les intrusions dans le réseau. Surveillez l'ensemble du trafic au périmètre de l'environnement des données de titulaires de cartes ainsi qu'aux points critiques de l'environnement des données de titulaires de cartes, et alertez le personnel en cas de suspicion de compromission. Maintenez à jour tous les moteurs, bases de référence et signatures de détection et de prévention des intrusions.	netfw-policy-rule-group-associated	Une politique de AWS Network Firewall définit la manière dont votre pare-feu surveille et gère le trafic dans un Amazon VPC. Vous configurez des groupes de règles avec ou sans état pour filtrer les paquets et les flux de trafic, et vous définissez la gestion du trafic par défaut.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.5	Déployez un mécanisme de détection des modifications (par exemple, des outils de surveillance de l'intégrité des fichiers) pour alerter le personnel en cas de modification non autorisée (y compris les ajouts et les suppressions) des fichiers système, des fichiers de configuration ou des fichiers de contenu critiques ; et configurez le logiciel pour qu'il effectue des comparaisons des fichiers critiques au moins une fois par semaine.	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
11.5	Déployez un mécanisme de détection des modifications (par exemple, des outils de surveillance de l'intégrité des fichiers) pour alerter le personnel en cas de modification non autorisée (y compris les ajouts et les suppressions) des fichiers système, des fichiers de configura tion ou des fichiers de contenu critiques ; et configurez le logiciel pour qu'il effectue des comparaisons des fichiers critiques au moins une fois par semaine.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for PCI DSS 3.2.1.

Bonnes pratiques de fonctionnement pour les ressources accessibles au public

Ce pack de conformité permet d'identifier les ressources susceptibles d'être accessibles au public.

Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les ressources accessibles au public.

Bonnes pratiques de fonctionnement pour le cadre de cybersécurité RBI pour les UCB

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le cadre de cybersécurité de la Reserve Bank of India (RBI) pour les banques coopératives urbaines (UCB) et les règles de AWS configuration gérées. Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs cadres de cybersécurité RBI pour les contrôles UCB. Un cadre de cybersécurité de la RBI pour les UCB peut être lié à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.1)	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir

ID du contrôle	AWS Règle de configuration	Conseils
		des configurations système détaillées, les niveaux de correctif du système d'exploit ation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
Annexe_I (1.1)	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.
Annexe_I (1.1)	ecr-private-tag-immutability-enabled	Activez l'immuabilité des balises Elastic Container Repository (ECR) pour éviter que les balises de vos images ECR ne soient écrasées. Jusqu'à présent, les balises pouvaient être écrasées, ce qui nécessitait l'utilisa tion de méthodes manuelles pour identifier une image de manière unique.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
Annexe_I (1.3)	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe_I (1.3)	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	api-gw-cache-enabled-and-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour le cache de votre environnement API Gateway. Étant donné que des données sensibles peuvent être capturées pour la méthode API, activez le chiffrement au repos pour protéger ces données.
Annexe_I (1.3)	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.
Annexe_I (1.3)	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes proviennent d'API Gateway.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
Annexe_I (1.3)	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.
Annexe_I (1.3)	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.
Annexe_I (1.3)	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	backup-recovery-point-encrypted	Assurez-vous que le chiffrement est activé pour vos points AWS de restauration Backup. Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Annexe_I (1.3)	codebuild-project-artifact-encryption	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild artefacts.
Annexe_I (1.3)	codebuild-project-s3-logs-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos AWS CodeBuild journaux stockés dans Amazon S3.
Annexe_I (1.3)	opensearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch Service.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
Annexe_I (1.3)	opensearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
Annexe_I (1.3)	dynamodb-table-encrypted-kms	Assurez-vous que le chiffrement est activé pour vos tables Amazon DynamoDB. Comme il peut y avoir des données sensibles au repos dans ces tables, activez le chiffrement au repos pour protéger ces données. Par défaut, les tables DynamoDB sont chiffrées à l'aide AWS d'une clé principale propre au client (CMK).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
Annexe_I (1.3)	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).
Annexe_I (1.3)	elasticsearch-encrypted-at-rest	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos domaines Amazon OpenSearch OpenSearch Service (Service).

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	elasticsearch-node-to-node-encryption-check	Assurez-vous que node-to-node le chiffrement pour Amazon OpenSearch Service est activé. ode-to-node Le chiffrement N active le chiffrement TLS 1.2 pour toutes les communications au sein d'Amazon Virtual Private Cloud (Amazon VPC). Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe_I (1.3)	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing . Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffreme nt en transit pour protéger ces données.
Annexe_I (1.3)	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
Annexe_I (1.3)	kms-cmk-not-scheduled-for-d eletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principal es du client (CMK) nécessair es n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppressi on est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	rds-snapshot-encrypted	Assurez-vous que le chiffrement est activé pour vos instantanés Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos, activez le chiffrement au repos pour protéger ces données.
Annexe_I (1.3)	rds-storage-encrypted	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos instances Amazon Relational Database Service (Amazon RDS). Comme il peut y avoir des données sensibles au repos dans les instances Amazon RDS, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe_I (1.3)	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessitent un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
Annexe_I (1.3)	s3-bucket-ssl-requests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	sagemaker-endpoint-configuration-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker terminal. Étant donné que les données sensibles peuvent exister au repos sur le SageMaker terminal, activez le chiffrement au repos pour protéger ces données.
Annexe_I (1.3)	sagemaker-notebook-instance-kms-key-configured	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre SageMaker ordinateur portable. Étant donné que des données sensibles peuvent exister au repos dans le SageMaker bloc-notes, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.
Annexe_I (1.3)	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibl es au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe_I (1.3)	ebs-snapshot-public-restora ble-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurables publiquement. Les instantanés des volumes EBS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
Annexe_I (1.3)	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearc h OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibles au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
Annexe_I (1.3)	no-unrestricted-route-to-igw	Assurez-vous que les tables de routage Amazon EC2 ne disposent pas de routes illimitées vers une passerelle Internet. La suppression ou la limitation de l'accès à Internet pour les charges de travail au sein des réseaux Amazon VPC peut réduire les accès imprévus au sein de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	redshift-cluster-kms-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement avec le service de gestion des AWS clés (AWS KMS) est activé pour votre cluster Amazon Redshift. Comme il peut y avoir des données sensibles au repos dans les clusters Redshift, activez le chiffrement au repos pour protéger ces données.
Annexe_I (1.3)	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involonta ire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiquement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.
Annexe_I (1.3)	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressource s dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirecti onnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Annexe_I (1.3)	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.
Annexe_I (1.3)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (1.3)	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Annexe_I (1.3)	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
Annexe_I (1.3)	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (5.1)	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibi lité, compromettre la sécurité ou consommer des ressource s excessives dans votre environnement.
Annexe_I (5.1)	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissa nt un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreind re l'accès à distance à vos AWS ressources.
Annexe_I (5.1)	waf-regional-rule-not-empty	Assurez-vous que votre AWS WAF possède une règle qui n'est pas vide. Une règle sans conditions peut entraîner un comportement involontaire.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (5.1)	waf-regional-rulegroup-not-empty	Assurez-vous que votre AWS WAF possède un groupe de règles qui n'est pas vide. Un groupe de règles vide peut entraîner un comportement involontaire.
Annexe_I (5.1)	waf-regional-webacl-not-empty	Une ACL Web attachée à un AWS WAF peut contenir un ensemble de règles et de groupes de règles pour inspecter et contrôler les requêtes Web. Si une liste ACL web est vide, le trafic web n'est pas détecté ni traité par le WAF.
Annexe_I (5.1)	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (5.1)	api-gw-associated-with-waf	AWS Le WAF vous permet de configurer un ensemble de règles (appelé liste de contrôle d'accès Web (ACL Web)) qui autorisent, bloquent ou comptent les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Assurez-vous que votre étape Amazon API Gateway est associée à une liste ACL Web WAF pour la protéger contre les attaques malveillantes
Annexe_I (5.1)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (5.1)	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (6)	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.
Annexe_I (6)	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (6)	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.
Annexe_I (6)	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (6)	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (6)	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automated SnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe_I (6)	vuln-management-plan-exists (vérification du processus)	Veillez à ce qu'un plan de gestion des vulnérabilités soit élaboré et mis en œuvre afin de disposer de processus officiellement définis pour remédier aux vulnérabilités dans votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisat ions d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
Annexe_I (7.1)	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.1)	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
Annexe_I (7.1)	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.1)	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.2)	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe_I (7.3)	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
Annexe_I (7.4)	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
Annexe_I (7.4)	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
Annexe_I (7.4)	cloudtrail-s3-dataevents-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
Annexe_I (7.4)	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.
Annexe_I (7.4)	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatch ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génération fournissent des informations détaillées sur votre projet de génération.
Annexe_I (7.4)	opensearch-audit-logging-enabled	Assurez-vous que la journalisation des audits est activée sur vos domaines Amazon OpenSearch Service. La journalisation des audits vous permet de suivre l'activité des utilisateurs sur vos OpenSearch domaines, notamment les réussites et les échecs d'authentification, les demandes OpenSearch, les modifications d'index et les requêtes de recherche entrantes.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
Annexe_I (7.4)	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD _TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région sans avoir à faire quoi que ce soit.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.
Annexe_I (7.4)	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.
Annexe_I (7.4)	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistr ent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (7.4)	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configura tions requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informati ons sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDb Encrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.
Annexe_I (10.2)	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibili sation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.
Annexe_I (12)	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.
Annexe_I (12)	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegard e. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entrepris e et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyUnit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisation. Les sauvegardes automatiques peuvent constituer une protection contre la perte de données. En cas de défaillance, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.
Annexe_I (12)	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.
Annexe_I (12)	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	AWS Règle de configuration	Conseils
Annexe_I (12)	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartim ent Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for RBI Cyber Security Framework for UCBs.

Bonnes pratiques de fonctionnement pour RBI MD-ITF

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre la Direction principale de la Reserve Bank of India (RBI) — Information Technology Framework et les règles de configuration AWS gérées.

Chaque règle de configuration s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles RBI Master Direction — Information Technology Framework. Un contrôle RBI MD-ITF peut être associé à plusieurs règles de configuration. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (a)	Identification et classification des actifs d'information.	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
3.1 (a)	Identification et classification des actifs d'information.	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.
3.1 (a)	Identification et classification des actifs d'information.	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppression lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (a)	Identification et classification des actifs d'information.	ecr-private-tag-immutability-enabled	Activez l'immuabilité des balises Elastic Container Repository (ECR) pour éviter que les balises de vos images ECR ne soient écrasées. Jusqu'à présent, les balises pouvaient être écrasées, ce qui nécessitait l'utilisation de méthodes manuelles pour identifier une image de manière unique.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
3.1 (c)	Contrôle d'accès basé sur les rôles	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).
3.1 (c)	Contrôle d'accès basé sur les rôles	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
3.1 (c)	Contrôle d'accès basé sur les rôles	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (c)	Contrôle d'accès basé sur les rôles	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
3.1 (c)	Contrôle d'accès basé sur les rôles	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (g)	Gestion des incidents	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (g)	Gestion des incidents	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (g)	Gestion des incidents	alb-waf-enabled	Assurez-vous que AWS le WAF est activé sur les Elastic Load Balancers (ELB) pour protéger les applications Web. Un WAF aide à protéger vos applications Web ou API contre les menaces Web courantes. Ces attaques web peuvent affecter la disponibilité, compromettre la sécurité ou consommer des ressources excessives dans votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (g)	Gestion des incidents	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (g)	Gestion des incidents	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
3.1 (h)	Journaux de suivi	api-gw-execution-logging-enabled	La journalisation d'API Gateway affiche des vues détaillées des utilisateurs qui ont accédé à l'API et de la manière dont ils y ont accédé. Ces informations offrent une visibilité sur les activités des utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralis ée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activit é des appels d'API au sein de votre Compte AWS.
3.1 (h)	Journaux de suivi	codebuild-project-logging-enabled	Assurez-vous que la journalisation AWS CodeBuild du projet est activée afin que les journaux de sortie de votre build soient envoyés à Amazon CloudWatc h ou à Amazon Simple Storage Service (Amazon S3). Les journaux de résultats de génératio n fournissent des informations détaillée s sur votre projet de génération.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	opensearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. OpenSearch Les journaux des erreurs de service peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.
3.1 (h)	Journaux de suivi	redshift-audit-logging-enabled	Pour recueillir des informations sur les connexions et les activités des utilisateurs sur votre cluster Amazon Redshift, assurez-vous que la journalisation des audits est activée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifie r les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistr ement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	cloudtrail-s3-data events-enabled	La collecte d'événements de données Simple Storage Service (Amazon S3) aide à détecter toute activité anormale. Les détails incluent les Compte AWS informations qui ont accédé à un compartiment Amazon S3, l'adresse IP et l'heure de l'événement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	cw-loggroup-retention-period-check	Assurez-vous que la durée minimale de conservation des données des journaux d'événements pour vos groupes de journaux est suffisante pour faciliter le dépannage et les enquêtes judiciaires. Le manque de données disponibles dans les journaux d'événements passés complique la reconstitution et l'identification des événements potentiellement malveillants.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	elasticsearch-logs-to-cloudwatch	Assurez-vous que les journaux d'erreurs sont activés sur les domaines Amazon OpenSearch Service et qu'ils sont transmis à Amazon CloudWatch Logs à des fins de conservation et de réponse. Les journaux d'erreurs de domaine peuvent faciliter les audits de sécurité et d'accès, ainsi que le diagnostic des problèmes de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	elb-logging-enabled	L'activité Elastic Load Balancing est un point de communication central au sein d'un environnement. Assurez-vous que la journalisation ELB est activée. Les données collectées fournissent des informations détaillées sur les demandes envoyées à l'ELB. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	multi-region-cloudtrail-enabled	AWS CloudTrail enregistre les actions AWS de la console de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. CloudTrail fournira les fichiers journaux de toutes les AWS régions à votre compartiment S3 si MULTI_REGION_CLOUD_TRAIL_ENABLED est activé. De plus, lors du AWS lancement d'une nouvelle région, le même parcours CloudTrail sera créé dans la nouvelle région. Par conséquent, vous recevrez des fichiers journaux contenant l'activité de l'API pour la nouvelle région

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			sans avoir à faire quoi que ce soit.
3.1 (h)	Journaux de suivi	rds-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, assurez-vous que la journalisation Amazon Relational Database Service (Amazon RDS) est activée. Avec la journalisation Amazon RDS, vous pouvez capturer des événements tels que des connexions, des déconnexions, des requêtes ou des tables interrogées.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveille r le réseau pour détecter d'éventue ls événements de cybersécurité. Les événement s sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur , le nom du compartim ent, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informations détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différents composants du flux IP, y compris la source, la destination et le protocole.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	wafv2-logging-enabled	Pour faciliter la journalisation et la surveillance au sein de votre environnement, activez la journalisation AWS WAF (V2) sur les ACL Web régionales et mondiales. AWS La journalisation WAF fournit des informations détaillées sur le trafic analysé par votre ACL Web. Les journaux enregistrent l'heure à laquelle AWS WAF a reçu la demande de votre AWS ressource, des informations sur la demande et une action pour la règle à laquelle chaque demande correspondait.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (h)	Journaux de suivi	redshift-cluster-configuration-check	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos clusters Amazon Redshift. Vous devez également vous assurer que les configurations requises sont déployées sur les clusters Amazon Redshift. La journalisation des audits doit être activée pour fournir des informations sur les connexions et les activités de l'utilisateur dans la base de données. Cette règle nécessite qu'une valeur soit définie pour clusterDbEncrypted (Config Default : TRUE) et LoggingEnabled (Config Default : TRUE). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (i)	Infrastructure à clés publiques (ICP)	acm-certificate-expiration-check	Assurez-vous que l'intégrité du réseau est protégée en vous assurant que les certificats X509 sont émis par AWS ACM. Ces certificats doivent être valides et non expirés. Cette règle nécessite une valeur pour daysToExpiration (valeur des meilleures pratiques de sécuritéAWS fondamentales : 90). La valeur réelle doit refléter les politiques de votre organisation.
3.1 (i)	Infrastructure à clés publiques (ICP)	alb-http-drop-invalid-header-enabled	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés pour ne pas prendre en compte les en-têtes http. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (i)	Infrastructure à clés publiques (ICP)	alb-http-to-https-redirection-check	Pour protéger les données en transit, assurez-vous que votre Application Load Balancer redirige automatiquement les requêtes HTTP non chiffrées vers HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1 (i)	Infrastructure à clés publiques (ICP)	api-gw-ssl-enabled	Assurez-vous que les étapes de l'API REST Amazon API Gateway sont configurées avec des certificats SSL pour permettre aux systèmes backend d'authentifier que les demandes provienne nt d'API Gateway.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (i)	Infrastructure à clés publiques (ICP)	opensearch-https-required	Étant donné que des données sensibles peuvent exister et pour protéger les données en transit, assurez-vous que le protocole HTTPS est activé pour les connexions à vos domaines Amazon OpenSearch Service.
3.1 (i)	Infrastructure à clés publiques (ICP)	elbv2-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (i)	Infrastructure à clés publiques (ICP)	elb-acm-certificate-required	Comme il peut y avoir des données sensibles et pour protéger les données en transit, assurez-vous que le chiffrement est activé pour votre Elastic Load Balancing. Utilisez AWS Certificate Manager pour gérer, fournir et déployer des certificats SSL/TLS publics et privés avec des AWS services et des ressources internes.
3.1 (i)	Infrastructure à clés publiques (ICP)	elb-tls-https-listeners-only	Assurez-vous que vos équilibreurs de charge Elastic Load Balancing (ELB) sont configurés avec des écouteurs SSL ou HTTPS. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.1 (i)	Infrastructure à clés publiques (ICP)	redshift-require-tls-ssl	Assurez-vous que vos clusters Amazon Redshift nécessite nt un chiffrement TLS/SSL pour se connecter aux clients SQL. Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.
3.1 (i)	Infrastructure à clés publiques (ICP)	s3-bucket-ssl-requ ests-only	Pour protéger les données en transit, assurez-vous que vos compartiments Amazon Simple Storage Service (Amazon S3) exigent que les demandes utilisent Secure Socket Layer (SSL). Comme il peut y avoir des données sensibles, activez le chiffrement en transit pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Vulnerability Management	elastic-beanstalk-managed-updates-enabled	L'activation des mises à jour de plateforme gérées pour un environnement Amazon Elastic Beanstalk garantit l'installation des derniers correctifs, mises à jour et fonctionnalités de la plateforme disponibles pour l'environnement. La sécurisation des systèmes passe par la mise à jour de l'installation des correctifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Vulnerability Management	rds-automatic-minor-version-upgrade-enabled	Activez les mises à niveau automatiques des versions mineures sur vos instances Amazon Relational Database Service (RDS) pour vous assurer que les dernières mises à jour mineures du système de gestion de base de données relationnelle (RDBMS) sont installées, lesquelles peuvent inclure des correctifs de sécurité et des correctifs de bogues.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Vulnerability Management	redshift-cluster-maintenancesettings-check	Cette règle garantit que les clusters Amazon Redshift disposent des paramètres préférés de votre organisation. Plus précisément, qu'ils disposent de fenêtres de maintenance préférées et de périodes de conservation des instantanés automatisées pour la base de données. Cette règle vous oblige à définir le allowVersionUpgrade. Par défaut, la valeur est true. Il vous permet également de définir éventuellement le preferredMaintenanceWindow (la valeur par défaut est samedi : 16h00 - samedi : 16h30) et la automatedSnapshotRetention période (la valeur par défaut est 1). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Vulnerability Management	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Vulnerability Management	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Vulnerability Management	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3.3	Vulnerability Management	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,5	Plan de gestion des cybercrises	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,5	Plan de gestion des cybercrises	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,5	Plan de gestion des cybercrises	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,5	Plan de gestion des cybercrises	ec2-managedinstance-association-compliance-status-check	Utilisez AWS les associations de Systems Manager pour vous aider à inventorier les plateformes logicielles et les applications au sein d'une organisation. AWS Systems Manager attribue un état de configuration à vos instances gérées et vous permet de définir des niveaux de référence pour les niveaux de correctifs du système d'exploitation, les installations de logiciels, les configurations d'applications et d'autres informations relatives à votre environnement.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,5	Plan de gestion des cybercrises	ec2-managedinstance-patch-compliance-status-check	Activez cette règle pour faciliter l'identification et la documentation des vulnérabilités d'Amazon Elastic Compute Cloud (Amazon EC2). La règle vérifie si les correctifs d'instance Amazon EC2 sont conformes dans AWS Systems Manager conformément aux politiques et procédures de votre entreprise.
3.9	Évaluation des risques informatiques	annual-risk-assessment-performed (vérification du processus)	Effectuez une évaluation annuelle des risques au sein de votre organisation. Les évaluations des risques peuvent aider à déterminer la probabilité et l'impact des risques et/ou des vulnérabilités identifiés sur une organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
3,12	Entraînement	security-awareness-program-exists (vérification du processus)	Élaborez et maintenez un programme de sensibilisation à la sécurité pour votre organisation. Les programmes de sensibilisation à la sécurité visent à informer les employés sur la façon de protéger leur organisation contre divers incidents ou atteintes à la sécurité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (g)	Analyse des fraudes - Analyse des transactions suspectes, détournements de fonds, vols ou soupçons de blanchiment d'argent, détournement d'actifs, manipulations de documents financiers, etc. L'obligation réglementaire de signaler les fraudes à la RBI devrait être axée sur le système.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	elb-deletion-prote ction-enabled	Cette règle garantit que la protection contre la suppressi on est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidente lle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	clb-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibi lité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiq uement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibi lité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	lambda-vpc-multi-az-check	Si votre fonction AWS Lambda est configuré e pour se connecter à un cloud privé virtuel (VPC) dans votre compte, déployez la fonction AWS Lambda dans au moins deux zones de disponibi lité différentes afin de vous assurer que votre fonction est disponible pour traiter les événements en cas d'interruption de service dans une seule zone.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppressi on est activée sur les instances Amazon Relationa l Database Service (Amazon RDS). Utilisez la protectio n contre la suppressi on pour empêcher la suppression accidente lle ou malveilla nte des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	s3-bucket-default-lock-enabled	Assurez-vous que le verrouillage est activé par défaut dans votre compartim ent Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments S3, appliquez le verrouill age d'objet au repos pour protéger ces données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondant s peuvent être mis en œuvre pour répondre aux exigences de résilienc e. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendra it indisponible. Pour bénéficier d'une protection contre la perte de connectiv ité en cas d'indispo nibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilib reur de charge envoie périodiqu ement des pings, effectue des tentative s de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	dynamodb-throughpu t-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d 'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informati ons pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuell ement les paramètre s AccountRCU (ThresholdPercenta ge Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	lambda-dlq-check	Activez cette règle pour notifier le personnel concerné par l'intermédiaire d'Amazon Simple Queue Service (Amazon SQS) ou d'Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une fonction.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	beanstalk-enhanced -health-reporting- enabled	AWS Les rapports de santé améliorés d'Elastic Beanstalk permettent de réagir plus rapidement aux modifications de l'état de santé de l'infrast ructure sous-jacente. Ces modifications peuvent entraîner un manque de disponibi lité de l'application. Les rapports d'état améliorés Elastic Beanstalk fournisse nt un descripteur d'état permettant d'évaluer la gravité des problèmes identifiés et d'identifier les causes possibles à étudier.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	rds-enhanced-monit oring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibi lité d'Amazon RDS. Vous disposez ainsi d'une visibilit é détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploieme nt Multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	ebs-optimized-inst ance	Une instance optimisée dans Amazon Elastic Block Store (Amazon EBS) fournit une capacité supplémentaire dédiée aux opérations d'E/S d'Amazon EBS. Cette optimisation offre les performances les plus efficaces pour vos volumes EBS en minimisant les conflits entre les opérations d'E/S d'Amazon EBS et le trafic restant de votre instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (h)	Analyse des capacités et des performan ces des systèmes de sécurité informatique.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (i)	Signalement des incidents, leur impact et les mesures prises pour que de tels événements ne se reproduisent plus à l'avenir.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
4.4 (i)	Signalement des incidents, leur impact et les mesures prises pour que de tels événements ne se reproduisent plus à l'avenir.	guardduty-non-archived-findings	Amazon vous GuardDuty aide à comprendre l'impact d'un incident en classant les résultats par gravité : faible, moyenne et élevée. Vous pouvez utiliser ces classifications pour déterminer les stratégies et les priorités de correction. Cette règle vous permet de définir éventuellement daysLowSev (Config Default : 30), daysMediumSev (Config Default : 7) et daysHighSev (Config Default : 1) pour les résultats non archivés, comme l'exigent les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	dynamodb-autoscali ng-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiq uement aux modèles de trafic réels. Cela permet à une table ou à un index secondair e global d'augment er sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	aurora-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Aurora font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegard e est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e. Cette règle vous permet de définir les paramètres requiredFrequencyV alue (Config par défaut : 1), requiredR etentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commerciaux critiques et leurs centres de données.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	cmk-backing-key-rotation-enabled	Activez la rotation des clés pour vous assurer que les clés sont pivotées une fois qu'elles ont atteint la fin de leur période de chiffrement.
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transacti ons. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiqu es pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commerciaux critiques et leurs centres de données.	ec2-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos ressources Amazon Elastic Compute Cloud (Amazon EC2) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commerciaux critiques et leurs centres de données.	fsx-resources-protected-by-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon FSx font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos instances Amazon Relationa l Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegard e entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegard e.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	redshift-backup-en abled	Pour faciliter les processus de sauvegarde des données, assurez-v ous que vos clusters Amazon Redshift disposent d'instant anés automatisés. Lorsque les instantan és automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modificat ion des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
6.3	Les NBFC doivent prendre en compte la nécessité de mettre en place des sites de sauvegarde pour leurs systèmes commercia ux critiques et leurs centres de données.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartim ents Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	dynamodb-autoscaling-enabled	Amazon DynamoDB Auto Scaling AWS utilise le service Application Auto Scaling pour ajuster la capacité de débit allouée afin de répondre automatiquement aux modèles de trafic réels. Cela permet à une table ou à un index secondaire global d'augmenter sa capacité de lecture/d'écriture approvisionnée afin de gérer les hausses soudaines de trafic sans limitation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	elb-cross-zone-load-balancing-enabled	Activez l'équilibrage de charge entre zones pour vos équilibre urs de charge Elastic Load Balancing (ELB) afin de maintenir une capacité et une disponibilité adéquates. L'équilib rage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instanc es dans chaque zone de disponibilité activée. Cela améliore également la capacité de votre applicati on à gérer la perte d'une ou de plusieurs instances.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	elb-deletion-protection-enabled	Cette règle garantit que la protection contre la suppression est activée pour Elastic Load Balancing. Utilisez cette fonctionnalité pour empêcher la suppression accidentelle ou malveillante de votre équilibreur de charge, ce qui pourrait entraîner une perte de disponibilité pour vos applications.
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	clb-multiple-az	Elastic Load Balancing (ELB) distribue automatiquement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	elbv2-multiple-az	Elastic Load Balancing (ELB) distribue automatiquement votre trafic entrant sur plusieurs cibles telles que des instances EC2, des conteneurs et des adresses IP), dans une zone de disponibilité. Pour garantir une disponibilité élevée, vérifiez que votre ELB a enregistré des instances provenant de plusieurs zones de disponibilité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	lambda-vpc-multi-az-check	Si votre fonction AWS Lambda est configuré e pour se connecter à un cloud privé virtuel (VPC) dans votre compte, déployez la fonction AWS Lambda dans au moins deux zones de disponibi lité différentes afin de vous assurer que votre fonction est disponible pour traiter les événements en cas d'interruption de service dans une seule zone.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	rds-instance-deletion-protection-enabled	Assurez-vous que la protection contre la suppression est activée sur les instances Amazon Relational Database Service (Amazon RDS). Utilisez la protection contre la suppression pour empêcher la suppression accidentelle ou malveillante des instances Amazon RDS, ce qui pourrait entraîner une perte de disponibilité pour vos applications.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	rds-multi-az-support	La prise en charge multi-AZ dans Amazon Relationa l Database Service (Amazon RDS) offre une disponibi lité et une durabilit é améliorées pour les instances de base de données. Lorsque vous mettez en service une instance de base de données multi-AZ, Amazon RDS crée automatiquement une instance de base de données principale et réplique de manière synchrone les données vers une instance de secours dans une autre zone de disponibi lité. Chaque zone de disponibilité fonctionne sur sa propre infrastru cture physiquem ent distincte et indépendante, et est conçue pour être hautement fiable. En

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			cas de défaillance de l'infrastructure, Amazon RDS effectue un basculement automatique vers l'instance de secours afin que vous puissiez poursuivre les opérations de base de données dès que le basculement est terminé.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	vpc-vpn-2-tunnels-up	Des tunnels Site-to-Site VPN redondants peuvent être mis en œuvre pour répondre aux exigences de résilience. Deux tunnels sont utilisés pour garantir la connectivité au cas où l'une des connexions Site-to-Site VPN deviendrait indisponible. Pour bénéficier d'une protection contre la perte de connectivité en cas d'indisponibilité de votre passerelle client, vous pouvez configurer une seconde connexion Site-to-Site VPN vers votre réseau Amazon Virtual Private Cloud (Amazon VPC) et votre passerelle privée virtuelle en ajoutant une seconde passerelle client.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	autoscaling-group-elb-healthcheck-required	La surveillance de l'état Elastic Load Balancer (ELB) pour les groupes Auto Scaling Amazon Elastic Compute Cloud (Amazon EC2) permet de maintenir une capacité et une disponibilité adéquates. L'équilibreur de charge envoie périodiquement des pings, effectue des tentatives de connexion ou adresse des demandes pour tester l'état des instances Amazon EC2 dans un groupe Auto Scaling. Si une instance ne renvoie pas de rapport, le trafic est envoyé à une nouvelle instance Amazon EC2.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	dynamodb-throughput-limit-check	Activez cette règle pour vous assurer que la capacité de débit allouée est vérifiée sur vos tables Amazon DynamoDB. Il s'agit du volume d'activité de lecture/d'écriture que chaque table peut prendre en charge. DynamoDB utilise ces informations pour réserver des ressources système suffisantes pour répondre à vos exigences de débit. Cette règle génère une alerte lorsque le débit approche de la limite maximale pour le compte d'un client. Cette règle vous permet de définir éventuellement les paramètres AccountRCU (ThresholdPercentage Config Default : 80) et AccountWCU ThresholdPercentage (Config Default : 80). Les valeurs réelles

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			doivent refléter les politiques de votre organisation.
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphique s de surveillance toutes les minutes pour l'instance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiels liés à la cybersécurité en utilisant des flux de renseignements sur les menaces. Il s'agit notamment de listes d'adresse s IP malveillantes et de l'apprentissage automatique pour identifier les activités inattendues, non autorisées et malveilla ntes au sein de votre environnement AWS cloud.
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	lambda-concurrency-check	Cette règle assure que les limites de simultanéité élevées et basses d'une fonction Lambda ont été définies. Elle permet de référence r le nombre de demandes auxquelles votre fonction répond à un moment donné.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	rds-enhanced-monitoring-enabled	Activez Amazon Relational Database Service (Amazon RDS) pour surveiller la disponibilité d'Amazon RDS. Vous disposez ainsi d'une visibilité détaillée sur l'état de vos instances de base de données Amazon RDS. Lorsque le stockage Amazon RDS utilise plusieurs appareils physiques sous-jacents, Enhanced Monitoring collecte les données pour chaque appareil. En outre, lorsque l'instance de base de données Amazon RDS est exécutée dans le cadre d'un déploiement Multi-AZ, les données de chaque appareil sur l'hôte secondaire sont collectées, ainsi que les métriques de l'hôte secondaire.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.1	Les systèmes informatiques devraient être progressivement renforcés à mesure que la taille et la complexité des opérations des NBFC augmentent.	securityhub-enabled	AWS Security Hub permet de surveille r le personnel, les connexions, les appareils et les logiciels non autorisés . AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	dms-replication-not-public	Gérez l'accès au AWS cloud en vous assurant que les instances de réplication DMS ne sont pas accessibles au public. Les instances de réplication DMS peuvent contenir des informations sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	ebs-snapshot-public-restorable-check	Gérez l'accès au AWS cloud en vous assurant que les instantanés EBS ne sont pas restaurab les publiquement. Les instantanés des volumes EBS peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibles au public. Les instances Amazon EC2 peuvent contenir des informati ons sensibles, c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	elasticsearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch OpenSearch Service (Service) se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine de OpenSearch service au sein d'un Amazon VPC permet une communication sécurisée entre le OpenSearch service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerell e Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	emr-master-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les nœuds maîtres du cluster Amazon EMR ne sont pas accessibl es au public. Les nœuds principaux du cluster Amazon EMR peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphéri que NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminais on publics. Pour gérer correctement l'accès, les fonctions AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			Lambda doivent être attribuées à un VPC.
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	rds-instance-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relational Database Service (Amazon RDS) ne sont pas publiques. Les instances de base de données Amazon RDS peuvent contenir des informations sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	rds-snapshots-public-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les instances Amazon Relationa l Database Service (Amazon RDS) ne sont pas publiques . Les instances de base de données Amazon RDS peuvent contenir des informati ons sensibles, c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	redshift-cluster-public-access-check	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les clusters Amazon Redshift ne sont pas publics. Les clusters Amazon Redshift peuvent contenir des informations sensibles , c'est pourquoi des principes et un contrôle des accès sont requis pour ces comptes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreint s sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibi lité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètre s blockedPort1 à blockedPort5 (configuration par défaut : 20,21,338 9,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBucketsles paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	s3-bucket-public-read-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	sagemaker-notebook-no-direct-internet-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les SageMaker blocs-notes Amazon ne permettent pas un accès direct à Internet. En empêchant l'accès direct à Internet, vous pouvez empêcher les utilisateurs non autorisés d'accéder à des données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribue r à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressource s. AWS La restricti on de l'ensemble du trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	access-keys-rotated	Les informations d'identification sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformément à la politique de l'organisation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	emr-kerberos-enabled	Les autorisations d'accès peuvent être gérées et intégrées selon les principes du moindre privilège et de la séparatio n des tâches, en activant Kerberos pour les clusters Amazon EMR. Dans Kerberos, les services et utilisateurs qui ont besoin de s'authent ifier sont appelés principaux. Les principaux existent au sein d'un domaine Kerberos. Dans le domaine, un serveur Kerberos est connu sous le nom de centre de diffusion des clés (KDC). Il fournit aux principaux un moyen de s'authentifier. Le KDC s'authentifie en émettant des tickets d'authentification . Il gère une base de données des principaux au sein de son domaine, leurs mots de passe, ainsi

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			que d'autres informations administratives sur chaque principal.
8.l	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utilise r des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisat ions.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Fondational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	autoscaling-launch-config-public-ip-disabled	Si vous configurez vos interfaces réseau avec une adresse IP publique, les ressources associées à ces interfaces réseau sont accessibles depuis Internet. Les ressources EC2 ne doivent pas être accessibles au public, car cela pourrait permettre un accès imprévu à vos applications ou à vos serveurs.
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	ecs-task-definition-nonroot-user	Pour faciliter la mise en œuvre du principe du moindre privilège, assurez-vous qu'un utilisateur non root dispose d'un accès à vos définitions de tâches Amazon Elastic Container Service (Amazon ECS).

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	efs-access-point-enforce-root-directory	Utiliser un répertoire racine pour un point d'accès Amazon Elastic File System (Amazon EFS) permet de restreindre l'accès aux données en veillant à ce que les utilisateurs du point d'accès ne puissent accéder qu'aux fichiers du sous-répertoire spécifié.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	efs-access-point-enforce-user-identity	Pour faciliter la mise en œuvre du principe du moindre privilège , assurez-vous que l'application des utilisateurs est activée pour votre Amazon Elastic File System (Amazon EFS). Lorsque cette option est activée, Amazon EFS remplace les ID utilisateur et de groupe du client NFS par l'identité configurée sur le point d'accès pour toutes les opérations du système de fichiers et n'accorde l'accès qu'à cette identité d'utilisateur appliquée.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommandé d'utiliser des politiques IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public au niveau du compartiment.
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	subnet-auto-assign-public-ip-disabled	Gérez l'accès au AWS cloud en vous assurant qu'aucune adresse IP publique n'est automatiq uement attribuée aux sous-réseaux Amazon Virtual Private Cloud (VPC). Les instances Amazon Elastic Compute Cloud (EC2) lancées dans des sous-réseaux pour lesquels cet attribut est activé ont une adresse IP publique attribuée à leur interface réseau principale.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisa teur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Managemen t (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège . Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémen taire de protection, en plus des informati ons d'identification de connexion. En exigeant la MFA pour les utilisate urs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisate urs non autorisés d'accéder aux données sensibles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondament aux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	opensearch-in-vpc-only	Gérez l'accès au AWS cloud en vous assurant que les domaines Amazon OpenSearch Service se trouvent dans un Amazon Virtual Private Cloud (Amazon VPC). Un domaine Amazon OpenSearch Service au sein d'un Amazon VPC permet une communication sécurisée entre Amazon OpenSearch Service et les autres services au sein d'Amazon VPC sans avoir besoin d'une passerelle Internet, d'un appareil NAT ou d'une connexion VPN.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant le MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	secretsmanager-rotation-enabled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
8.I	Aspects fondamentaux de la sécurité comme les contrôles d'accès physiques /logiques et une politique de mots de passe bien définie.	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.II	Un rôle utilisateur bien défini.	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégre r le moindre privilège.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.II	Un rôle utilisateur bien défini.	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées . Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.II	Un rôle utilisateur bien défini.	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS base : 24) et MaxPasswordAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.II	Un rôle utilisateur bien défini.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches dans les autorisations et autorisations d'accès, en empêchant les politiques de contenir « Effect » : « Autoriser » avec « Action » : « * » plutôt que « Ressource » : « * ». Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.II	Un rôle utilisateur bien défini.	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.II	Un rôle utilisateur bien défini.	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Managemen t (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilège s excessifs.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.II	Un rôle utilisateur bien défini.	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisations d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifiées, vous devez les désactiver et/ou les supprimer afin de ne pas risquer d'enfreindre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.III	Un concept de Maker-checker pour réduire le risque d'erreur et d'abus et garantir la fiabilité des données/informations.	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	db-instance-backup-enabled	La fonctionnalité de sauvegarde d'Amazon RDS crée des sauvegardes de vos bases de données et de vos journaux de transactions. Amazon RDS crée automatiquement un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de cette dernière. Le système vous permet de définir des périodes de conservation spécifiques pour répondre à vos exigences de résilience.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	dynamodb-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos tables Amazon DynamoDB font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	dynamodb-pitr-enabled	Activez cette règle pour vérifier que les informations ont été sauvegardées. Il gère également les sauvegardes en s'assurant que la point-in-time restauration est activée dans Amazon DynamoDB. La récupération permet de maintenir des sauvegardes continues de votre table pour les 35 derniers jours.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	elasticache-redis-cluster-automatic-backup-check	Lorsque les sauvegardes automatiques sont activées, Amazon ElastiCache crée une sauvegarde du cluster quotidiennement. La sauvegarde peut être conservée pendant un nombre de jours défini par votre organisat ion. Les sauvegard es automatiques peuvent constituer une protection contre la perte de données. En cas de défaillan ce, vous pouvez créer un nouveau cluster, ce qui restaurera vos données à partir de la sauvegarde la plus récente.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	rds-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos instances Amazon Relational Database Service (Amazon RDS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	s3-bucket-replication-enabled	La réplication entre régions (CRR) Amazon Simple Storage Service (Amazon S3) facilite le maintien d'une capacité et d'une disponibilité adéquates. La CRR permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3 afin de garantir le maintien de la disponibilité des données.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	redshift-backup-enabled	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos clusters Amazon Redshift disposent d'instantanés automatisés. Lorsque les instantanés automatiques sont activés pour un cluster, Redshift prend régulièrement des instantanés de ce cluster. Par défaut, Redshift prend un instantané toutes les huit heures ou tous les 5 Go pour chaque nœud de modification des données, ou selon la première éventualité.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	backup-plan-min-frequency-and-min-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que votre plan AWS de sauvegarde est défini pour une fréquence et une rétention minimales. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir les paramètres requiredFrequencyValue (Config par défaut : 1), requiredRetentionDays (Config par défaut : 35) et requiredFrequencyU

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			nit (Config par défaut : jours). La valeur réelle doit refléter les exigences de votre organisation.
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	backup-recovery-point-manual-deletion-disabled	Assurez-vous que vos points AWS de restauration Backup sont associés à une politique basée sur les ressources qui empêche la suppression de points de restauration. L'utilisation d'une politique basée sur les ressources pour empêcher la suppression des points de récupération peut aider à empêcher les suppressions accidentelles ou intentionnelles.

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
8.IX	Dispositions pour la sauvegarde des données avec des tests réguliers.	backup-recovery-point-minimum-retention-check	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos points de restauration AWS Backup disposent d'une période de conservation minimale définie. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde. Cette règle vous permet de définir le paramètre requiredRetentionDays (par défaut de configuration : 35). La valeur réelle doit refléter les

ID du contrôle	Description du contrôle	AWS Règle de configuration	Conseils
			exigences de votre organisation.

Modèle

Le modèle est disponible sur GitHub : Operational Best Practices for RBI MD-ITF.

Bonnes pratiques de fonctionnement pour les services de sécurité, d'identité et de conformité

Ce pack de conformité contient des AWS Config règles basées sur les services de sécurité, d'identité et de conformité. Pour plus d'informations, consultez la section Sécurité, identité et conformité sur AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les services de sécurité, d'identité et de conformité.

Bonnes pratiques de fonctionnement pour le sans serveur

Ce pack de conformité contient des AWS Config règles basées sur des solutions sans serveur. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Operational Best Practices for Serverless.

Bonnes pratiques de fonctionnement pour les services de stockage

Ce pack de conformité contient des AWS Config règles basées sur les services de stockage. Pour plus d'informations, consultez Cloud Storage on AWS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour les services de stockage.

Bonnes pratiques de fonctionnement pour SWIFT CSP

Les packs de conformité fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide de AWS Config règles gérées ou personnalisées et d'actions correctives. AWS Config Les packs de conformité, en tant qu'exemples de modèle, ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si votre utilisation des services est conforme aux exigences légales et réglementaires applicables.

Vous trouverez ci-dessous un exemple de mappage entre le Customer Security Programme (CSP) de SWIFT et les règles de configuration gérées AWS . Chaque AWS Config règle s'applique à une AWS ressource spécifique et concerne un ou plusieurs contrôles SWIFT CSP. Un contrôle SWIFT CSP peut être lié à plusieurs AWS Config règles. Reportez-vous au tableau ci-dessous pour obtenir plus de détails et des conseils relatifs à ces mappages.

ID du contrôle	AWS Règle de configuration	Conseils
1.1	ec2-instance-managed-by-systems-manager	Un inventaire des plateformes logicielles et des applications au sein de l'organisation est possible en gérant les instances Amazon Elastic Compute Cloud (Amazon EC2) avec Systems AWS Manager. Utilisez AWS Systems Manager pour fournir des configurations système détaillées, les niveaux de correctif du système d'exploitation, le nom et le type de service, les installations

ID du contrôle	AWS Règle de configuration	Conseils
		logicielles, le nom, l'éditeur et la version de l'application, ainsi que d'autres informations sur votre environnement.
1.1	ec2-instance-no-public-ip	Gérez l'accès au AWS cloud en vous assurant que les instances Amazon Elastic Compute Cloud (Amazon EC2) ne sont pas accessibl es au public. Les instances Amazon EC2 peuvent contenir des informations sensibles , c'est pourquoi un contrôle des accès est requis pour ces comptes.
1.1	ec2-no-amazon-key-pair	Cette règle vérifie si les instances Amazon Elastic Compute Cloud (Amazon EC2) en cours d'exécution sont lancées à l'aide des paires de clés Amazon. Cela peut contribue r à réduire le risque de compromission des informati ons d'identification. Les instances Amazon EC2 sans paires de clés sont toujours accessibles via le gestionnaire de session ou une connexion SSH basée sur un navigateur via la console. AWS

ID du contrôle	AWS Règle de configuration	Conseils
1.1	ec2-instances-in-vpc	Déployez des instances Amazon Elastic Compute Cloud (Amazon EC2) au sein d'un réseau Amazon Virtual Private Cloud (Amazon VPC) pour permettre une communication sécurisée entre une instance et les autres services au sein du réseau Amazon VPC, sans nécessiter de passerelle Internet, de périphérique NAT ou de connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Attribuez des instances Amazon EC2 à un réseau Amazon VPC pour une gestion correcte des accès.

ID du contrôle	AWS Règle de configuration	Conseils
1.1	vpc-default-security-group-closed	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent contribuer à la gestion de l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS La restriction de tout le trafic sur le groupe de sécurité par défaut permet de restreindre l'accès à distance à vos AWS ressources.
1.1	vpc-network-acl-unused-check	Cette règle garantit que les listes de contrôle d'accès au réseau Amazon Virtual Private Cloud (VPC) sont utilisées. La surveillance des listes de contrôle d'accès réseau inutilisées peut faciliter l'inventaire et la gestion précis de votre environnement.

ID du contrôle	AWS Règle de configuration	Conseils
1.1	vpc-sg-open-only-to-authorized-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. En limitant l'accès aux ressources d'un groupe de sécurité depuis Internet (0.0.0.0/0), il est possible de contrôler l'accès à distance aux systèmes internes.

ID du contrôle	AWS Règle de configuration	Conseils
1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisat ions d'accès, en empêchant les politiques de contenir des actions bloquées sur toutes les AWS clés du Key Management Service. Avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches. Cette règle vous permet de définir le blockedActionsPatt erns paramètre. (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation

ID du contrôle	AWS Règle de configuration	Conseils
1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) peut vous aider à intégrer les principes du moindre privilège et de la séparation des tâches aux autorisations et autorisations d'accès, en garantissant que les groupes IAM comptent au moins un utilisateur. Placer les utilisateurs dans des groupes en fonction des autorisations ou des fonctions qui leur sont associées est une manière d'intégrer le moindre privilège.

ID du contrôle	AWS Règle de configuration	Conseils
1.2	iam-inline-policy-blocked-kms-actions	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée autorisant le blocage d'actions sur toutes les clés du service de gestion des clés. AWS AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions, la restauration, ainsi que la délégation de la gestion des autorisations. Cette règle vous permet de définir le blockedActionsPatterns paramètre . (Valeur des meilleures pratiques de sécuritéAWS fondamentales : KMS:Decrypt, kms : From). ReEncrypt Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1.2	iam-no-inline-policy-check	Assurez-vous qu'un utilisateur, un rôle IAM ou un groupe IAM (AWS Identity and Access Management) ne dispose pas d'une politique intégrée pour contrôler l'accès aux systèmes et aux actifs. AWS recommande d'utiliser des politiques gérées plutôt que des politiques intégrées. Les politiques gérées permettent la réutilisation, la gestion des versions et la restauration, ainsi que la délégation de la gestion des autorisations.
1.2	iam-user-no-policies-check	Cette règle garantit que les politiques AWS Identity and Access Management (IAM) ne sont associées qu'à des groupes ou à des rôles afin de contrôler l'accès aux systèmes et aux actifs. L'attribution de privilèges au niveau du groupe ou du rôle permet de réduire les risques qu'une identité reçoive ou conserve des privilèges excessifs.

ID du contrôle	AWS Règle de configuration	Conseils
1.2	restricted-ssh	Les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2) peuvent aider à gérer l'accès au réseau en fournissant un filtrage dynamique du trafic réseau entrant et sortant vers les ressources. AWS Ne pas autoriser le trafic entrant (ou distant) de 0.0.0.0/0 vers le port 22 sur vos ressources vous aide à restreindre l'accès à distance.
1.2	nacl-no-unrestricted-ssh-rdp	L'accès aux ports d'adminis tration des serveurs distants figurant dans vos listes de contrôle d'accès au réseau (NACL), tels que le port 22 (SSH) et le port 3389 (RDP), ne doit pas être accessible au public, car cela pourrait permettre un accès imprévu à des ressources au sein de votre VPC.

ID du contrôle	AWS Règle de configuration	Conseils
1.2	s3-bucket-acl-prohibited	Cette règle vérifie si les listes de contrôle d'accès (ACL) sont utilisées pour contrôler l'accès aux compartiments Amazon S3. Les ACL sont des mécanismes de contrôle d'accès existants pour les compartiments Amazon S3 antérieurs à AWS Identity and Access Management (IAM). Au lieu d'utiliser des listes ACL, il est recommand é d'utiliser des politique s IAM ou des politiques de compartiment S3 pour gérer plus facilement l'accès à vos compartiments S3.

ID du contrôle	AWS Règle de configuration	Conseils
1.2	s3-bucket-logging-enabled	La journalisation des accès au serveur Amazon Simple Storage Service (Amazon S3) permet de surveiller le réseau pour détecter d'éventuels événements de cybersécu rité. Les événements sont surveillés en capturant des enregistrements détaillés pour les demandes envoyées à un compartiment Amazon S3. Chaque enregistrement du journal des accès fournit des détails sur une unique demande d'accès. Les détails incluent le demandeur, le nom du compartiment, l'heure de la demande, l'action de la demande, l'état de la réponse et un code d'erreur, le cas échéant.
1.2	s3-bucket-policy-grantee-check	Gérez l'accès au AWS cloud en activant s3_ bucket_policy_grantee_check. Cette règle vérifie que l'accès accordé par le compartiment Amazon S3 est limité par les principaux, les utilisateurs fédérés, AWS les principaux de service, les adresses IP ou les identifiants Amazon Virtual Private Cloud (Amazon VPC) que vous fournissez.

ID du contrôle	AWS Règle de configuration	Conseils
1.2	sns-topic-message-delivery-notification-enabled	Pour répondre aux exigences de journalisation dans votre environnement, assurez-v ous que les notifications d'état de livraison sont activées pour vos rubriques Amazon Simple Notification Service (Amazon SNS). La journalis ation de l'état de livraison des messages permet d'obtenir une meilleure visibilit é opérationnelle, notamment : Savoir si un message a été livré au point de terminais on Amazon SNS, identifie r la réponse envoyée par le point de terminaison Amazon SNS à Amazon SNS, et déterminer le temps d'attente du message (le temps écoulé entre l'horodatage de la publication et le moment où le message est transmis à un point de terminaison Amazon SNS).

ID du contrôle	AWS Règle de configuration	Conseils
1.4	internet-gateway-authorized-vpc-only	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les passerelles Internet ne sont connectées qu'à Amazon Virtual Private Cloud (Amazon VPC) autorisé. Les passerelles Internet permettent un accès bidirectionnel à Internet depuis et vers le réseau Amazon VPC, ce qui peut potentiellement entraîner un accès non autorisé aux ressources Amazon VPC.

ID du contrôle	AWS Règle de configuration	Conseils
1.4	restricted-common-ports	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les ports courants sont restreints sur les groupes de sécurité Amazon Elastic Compute Cloud (Amazon EC2). Le fait de ne pas limiter l'accès aux ports à des sources fiables peut entraîner des attaques mettant en péril la disponibilité, l'intégrité et la confidentialité des systèmes. Cette règle vous permet éventuellement de définir les paramètres blockedPort1 à blockedPort5 (configuration par défaut : 20,21,3389,3306,4333). Les valeurs réelles doivent refléter les politiques de votre organisation.
1.4	lambda-function-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que les fonctions AWS Lambda ne sont pas accessibles au public. Un accès public peut potentiellement entraîner une dégradation de la disponibilité des ressources.

ID du contrôle	AWS Règle de configuration	Conseils
1.4	s3-account-level-public-access-blocks-periodic	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisateurs distants non autorisés en empêchant l'accès public. Cette règle vous permet de définir éventuellement les paramètres ignorePublicAcls (Config Default : True), blockPublicPolicy (Config Default : True), blockPublicAcls (Config Default : True) et restrictPublicBuckets les paramètres (Config Default : True). Les valeurs réelles doivent refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
1.4	s3-bucket-level-public-access-prohibited	Gérez l'accès aux ressources dans le AWS cloud en veillant à ce que les compartiments Amazon Simple Storage Service (Amazon S3) ne soient pas accessibles au public. Cette règle permet de protéger les données sensibles contre les utilisate urs distants non autorisés en empêchant l'accès public au niveau du compartiment.
1.4	s3-bucket-public-read-prohi bited	Gérez l'accès aux ressource s dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartim ents Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classific ation des données.

ID du contrôle	AWS Règle de configuration	Conseils
1.4	s3-bucket-public-write-prohibited	Gérez l'accès aux ressources dans le AWS cloud en autorisant uniquement les utilisateurs, les processus et les appareils autorisés à accéder aux compartiments Amazon Simple Storage Service (Amazon S3). La gestion des accès doit être cohérente avec la classification des données.
1.4	ssm-document-not-public	Assurez-vous que AWS les documents de Systems Manager (SSM) ne sont pas publics, car cela peut permettre un accès involontaire à vos documents SSM. Un document SSM public peut exposer des informations sur votre compte, vos ressources et vos processus internes.

ID du contrôle	AWS Règle de configuration	Conseils
2.3	ec2-imdsv2-check	Assurez-vous que la méthode Service des métadonnées d'instance Version 2 (IMDSv2) est activée pour protéger l'accès aux métadonné es d'instance Amazon Elastic Compute Cloud (Amazon EC2) et leur contrôle. La méthode IMDSv2 utilise des contrôles basés sur la session. Avec IMDSv2, des contrôles peuvent être mis en œuvre pour limiter les modifications apportées aux métadonnées des instances.
2.3	ec2-instance-multiple-eni-c heck	Cette règle vérifie si vos instances Amazon Elastic Compute Cloud (Amazon EC2) ont plusieurs ENI. Le fait d'avoir plusieurs ENI peut entraîner la création d'instances à double connexion, c'est-à-dire d'instances ayant plusieurs sous-réseaux. Cela peut ajouter à la complexité de la sécurité du réseau et introduir e des chemins et des accès non intentionnels au réseau.

ID du contrôle	AWS Règle de configuration	Conseils
2.3	ec2-token-hop-limit-check	Assurez-vous que la réponse HTTP PUT du service de métadonnées d'instance (IMDS) est limitée à l'instanc e Amazon Elastic Compute Cloud (Amazon EC2). Avec IMDSv2, la réponse PUT qui contient le jeton secret ne peut pas, par défaut, sortir de l'instance, car la limite des tronçons de la réponse Metadata est fixée à 1 (configuration par défaut). Si cette valeur est supérieure à 1, le jeton peut quitter l'instanc e EC2.
2.3	ec2-volume-inuse-check	Cette règle garantit que les volumes Amazon Elastic Block Store attachés aux instances Amazon Elastic Compute Cloud (Amazon EC2) sont marqués pour suppressi on lorsqu'une instance est résiliée. Si un volume Amazon EBS n'est pas supprimé lorsque l'instance à laquelle il est attaché est résiliée, cela peut enfreindre le concept de moindre fonctionn alité.

ID du contrôle	AWS Règle de configuration	Conseils
2.3	account-part-of-organizations	La gestion centralisée Comptes AWS au sein des AWS Organisations permet de garantir la conformité des comptes. L'absence de gouvernance centralisée des comptes peut entraîner des configurations de comptes incohérentes, ce qui peut exposer des ressources et des données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
2.3	lambda-inside-vpc	Déployez les fonctions AWS Lambda au sein d'un Amazon Virtual Private Cloud (Amazon VPC) pour une communication sécurisée entre une fonction et les autres services au sein d'Amazon VPC. Avec cette configuration, il n'est pas nécessaire d'avoir une passerelle Internet, un périphérique NAT ou une connexion VPN. Tout le trafic reste sécurisé dans le AWS cloud. En raison de leur isolement logique, les domaines résidant au sein d'un réseau Amazon VPC possèdent une couche de sécurité supplémentaire par rapport aux domaines qui utilisent des points de terminaison publics. Pour gérer correctement l'accès, les fonctions AWS Lambda doivent être attribuées à un VPC.

ID du contrôle	AWS Règle de configuration	Conseils
2.3	kms-cmk-not-scheduled-for-deletion	Pour protéger les données au repos, assurez-vous que la suppression des clés principales du client (CMK) nécessaires n'est pas planifiée dans le service de gestion des AWS clés (AWS KMS). La suppression de clés étant parfois nécessaire, cette règle peut aider à vérifier toutes les clés dont la suppression est prévue, au cas où la suppression d'une clé aurait été planifiée par inadvertance.
2.3	s3-bucket-versioning-enabled	La gestion des versions d'un compartiment Amazon Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d'un objet dans le même compartiment Amazon S3. Utilisez la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. La gestion des versions vous aide à récupérer facilement en cas d'action involontaire d'un utilisateur et de défaillance applicative.

ID du contrôle	AWS Règle de configuration	Conseils
2.3	secretsmanager-secret-unused	Si des informations d'identification non utilisées existent dans AWS Secrets Manager, vous devez les désactiver et/ou les supprimer, car cela pourrait violer le principe du moindre privilège. Cette règle vous permet de définir une valeur sur unusedForDays (Config Default : 90). La valeur réelle doit refléter les politiques de votre organisation.
2.5 A	ebs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos volumes Amazon Elastic Block Store (Amazon EBS) font partie d'un plan de sauvegarde. AWS AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegardes et vous permet de répondre aux exigences de conformité de votre entreprise et aux réglementations en matière de sauvegarde.

ID du contrôle	AWS Règle de configuration	Conseils
2.5 A	ec2-ebs-encryption-by-default	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS). Comme il peut y avoir des données sensibles au repos dans ces volumes, activez le chiffreme nt au repos pour protéger ces données.
2.5 A	efs-encrypted-check	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour votre Amazon Elastic File System (EFS).

ID du contrôle	AWS Règle de configuration	Conseils
2.5 A	efs-in-backup-plan	Pour faciliter les processus de sauvegarde des données, assurez-vous que vos systèmes de fichiers Amazon Elastic File System (Amazon EFS) font partie d'un plan de AWS sauvegarde. AWS Backup est un service de sauvegarde entièrement géré doté d'une solution de sauvegarde basée sur des règles. Cette solution simplifie la gestion de vos sauvegard es et vous permet de répondre aux exigences de conformit é de votre entreprise et aux réglementations en matière de sauvegarde.
2.5 A	encrypted-volumes	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos volumes Amazon Elastic Block Store (Amazon EBS).
2.5 A	kinesis-stream-encrypted	Comme il peut y avoir des données sensibles et pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos flux Amazon Kinesis Streams.

ID du contrôle	AWS Règle de configuration	Conseils
2.5 A	s3-bucket-server-side-encryption-enabled	Pour protéger les données au repos, assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans les compartiments Amazon S3, activez le chiffrement pour protéger ces données.
2.5 A	s3-default-encryption-kms	Assurez-vous que le chiffrement est activé pour vos compartiments Amazon Simple Storage Service (Amazon S3). Comme il peut y avoir des données sensibles au repos dans un compartiment Amazon S3, activez le chiffrement au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
2.5 A	sns-encrypted-kms	Pour protéger les données au repos, assurez-vous que vos rubriques Amazon Simple Notification Service (Amazon SNS) nécessitent un chiffrement à l' AWS aide du Key Management Service AWS (KMS). Comme il peut y avoir des données sensibles au repos dans les messages publiés, activez le chiffreme nt au repos pour protéger ces données.

ID du contrôle	AWS Règle de configuration	Conseils
4.1	iam-password-policy	Les identités et les informations d'identification sont émises, gérées et vérifiées conformément à une politique de mot de passe IAM organisationnelle. Ils respectent ou dépassent les exigences énoncées par le NIST SP 800-63 et par la norme AWS Foundational Security Best Practices en matière de robustesse des mots de passe. Cette règle vous permet de définir éventuellement RequireUppercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireLowercaseCharacters (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireSymbols (valeur des meilleures pratiques de sécurité de AWS base : vrai), RequireNumbers (valeur des meilleures pratiques de sécurité de AWS base : vrai), MinimumPasswordLength (valeur des meilleures pratiques de sécurité de AWS base : 14), PasswordReusePrevention (valeur des meilleures pratiques de sécurité de AWS

ID du contrôle	AWS Règle de configuration	Conseils
		base : 24) et MaxPasswo rdAge (valeur des meilleures pratiques de sécurité de AWS base : 90) pour votre IAM Politique de mot de passe. Les valeurs réelles doivent refléter les politiques de votre organisation.
4.1	access-keys-rotated	Les informations d'identif ication sont auditées pour les appareils, les utilisateurs et les processus autorisés en veillant à ce que les clés d'accès IAM soient alternées conformém ent à la politique de l'organis ation. La modification régulière des clés d'accès est une bonne pratique de sécurité. Cela permet de raccourcir la période pendant laquelle une clé d'accès est active et de réduire l'impact commercial en cas de compromission des clés. Cette règle nécessite une valeur de rotation des clés d'accès (configuration par défaut : 90). La valeur réelle doit refléter les politiques de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
4.2	iam-user-mfa-enabled	Activez cette règle pour restreindre l'accès aux ressources dans le AWS cloud. Cette règle garantit que l'authentification multifactorielle (MFA) est activée pour tous les utilisateurs. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. Réduisez les incidents de comptes compromis en imposant la MFA aux utilisateurs.
4.2	mfa-enabled-for-iam-console-access	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour tous les utilisateurs AWS d'Identity and Access Management (IAM) dotés d'un mot de passe de console. La MFA ajoute une couche supplémentaire de protection, en plus des informations d'identification de connexion. En exigeant la MFA pour les utilisateurs, vous pouvez réduire les incidents liés à des comptes compromis et empêcher les utilisateurs non autorisés d'accéder aux données sensibles.

ID du contrôle	AWS Règle de configuration	Conseils
4.2	root-account-hardware-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le matériel MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS

ID du contrôle	AWS Règle de configuration	Conseils
4.2	root-account-mfa-enabled	Gérez l'accès aux ressources dans le AWS cloud en vous assurant que le MFA est activé pour l'utilisateur root. L'utilisateur root est l'utilisateur disposant du plus haut niveau de privilèges dans un Compte AWS. La MFA ajoute une couche supplémentaire de protection pour les informations d'identification de connexion En exigeant l'authentification MFA pour l'utilisateur root, vous pouvez réduire le nombre d'incidents de compromission. Comptes AWS
5.1	ec2-instance-profile-attached	Les profils d'instance EC2 transmettent un rôle IAM à une instance EC2. L'association d'un profil d'instance à vos instances peut faciliter la gestion du moindre privilège et des autorisations.
5.1	iam-policy-no-statements-with-full-access	Assurez-vous que les actions IAM sont limitées aux seules actions nécessaires. Permettre aux utilisateurs d'avoir plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
5.1	iam-root-access-key-check	L'accès aux systèmes et aux actifs peut être contrôlé en vérifiant que l'utilisateur root ne dispose pas de clés d'accès associées à son AWS rôle Identity and Access Management (IAM). Assurez-vous que les clés d'accès root ont été supprimées. Créez et utilisez plutôt la fonction basée sur Comptes AWS les rôles pour intégrer le principe de moindre fonctionnalité.
5.1	iam-user-group-membership-check	AWS Identity and Access Management (IAM) peut vous aider à restreindre les autorisations et autorisations d'accès en vous assurant que les utilisateurs sont membres d'au moins un groupe. Accorder aux utilisateurs plus de privilèges que nécessaire pour effectuer une tâche peut enfreindre le principe du moindre privilège et de la séparation des tâches.

ID du contrôle	AWS Règle de configuration	Conseils
5.1	iam-user-unused-credentials-check	AWS Identity and Access Management (IAM) peut vous aider à obtenir des autorisations et des autorisat ions d'accès en vérifiant les mots de passe et les clés d'accès IAM qui ne sont pas utilisés pendant une période donnée. Si de telles informations d'identification non utilisées sont identifié es, vous devez les désactive r et/ou les supprimer afin de ne pas risquer d'enfrein dre le principe du moindre privilège. Cette règle vous oblige à définir une valeur sur maxCredentialUsage Age (Config Default : 90). La valeur réelle doit refléter les politique s de votre organisation.
5.4	secretsmanager-rotation-ena bled-check	Cette règle garantit que la rotation AWS des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiel lement réduire l'impact commercial s'il est compromis.

ID du contrôle	AWS Règle de configuration	Conseils
5.4	secretsmanager-scheduled-rotation-success-check	Cette règle garantit que AWS les secrets de Secrets Manager ont été correctement transférés conformément au calendrier de rotation. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis.
5.4	secretsmanager-secret-periodic-rotation	Cette règle garantit que AWS la rotation périodique des secrets de Secrets Manager est activée. La rotation régulière des secrets peut raccourcir la période pendant laquelle un secret est actif et potentiellement réduire l'impact commercial s'il est compromis. La valeur par défaut est 90 jours.

ID du contrôle	AWS Règle de configuration	Conseils
5.4	secretsmanager-using-cmk	Pour protéger les données au repos, assurez-vous que le chiffrement avec le AWS Key Management Service (AWS KMS) est activé pour les AWS secrets de Secrets Manager. Comme il peut y avoir des données sensibles au repos dans les secrets de Secrets Manager, activez le chiffrement au repos pour protéger ces données.
6.4	ec2-instance-detailed-monitoring-enabled	Activez cette règle pour améliorer la surveillance des instances Amazon Elastic Compute Cloud (Amazon EC2) sur la console Amazon EC2, qui affiche des graphiques de surveillance toutes les minutes pour l'instance.
6.4	cloudwatch-log-group-encrypted	Pour protéger les données sensibles au repos, assurez-vous que le chiffrement est activé pour vos Amazon CloudWatch Log Groups.

ID du contrôle	AWS Règle de configuration	Conseils
6.4	cloud-trail-cloud-watch-logs-enabled	Utilisez Amazon CloudWatch pour collecter et gérer de manière centralisée l'activité des événements du journal. L'inclusion de AWS CloudTrail données fournit des détails sur l'activité des appels d'API au sein de votre Compte AWS.
6.4	cloudtrail-enabled	AWS CloudTrail peut contribuer à la non-répudiation en enregistrant les actions de la console AWS de gestion et les appels d'API. Vous pouvez identifier les utilisateurs et la Comptes AWS personne qui a appelé un AWS service, l'adresse IP source à laquelle les appels ont été générés et les horaires des appels. Les détails des données capturées sont affichés dans le contenu de l' AWS CloudTrail enregistrement.
6.4	cloud-trail-encryption-enabled	Étant donné que des données sensibles peuvent exister et pour protéger les données au repos, assurez-vous que le cryptage est activé pour vos AWS CloudTrail pistes.

ID du contrôle	AWS Règle de configuration	Conseils
6.4	cloud-trail-log-file-validation-enabled	Utilisez la validation des fichiers AWS CloudTrail journaux pour vérifier l'intégrité des CloudTrail journaux. La validation du fichier journal permet de déterminer si un fichier journal a été modifié, supprimé ou inchangé après CloudTrail sa livraison. Cette fonctionnalité est créée grâce à des algorithmes standard du secteur : SHA-256 pour le hachage et SHA-256 avec RSA pour la signature numérique. Il est donc impossible, sur le plan informatique, de modifier, de supprimer ou de falsifier des fichiers CloudTrail journaux sans détection.
6.4	ec2-stopped-instance	Activez cette règle pour faciliter la configuration de référence des instances Amazon Elastic Compute Cloud (Amazon EC2) en vérifiant si les instances Amazon EC2 ont été arrêtées pendant un nombre de jours supérieur au nombre autorisé, conformément aux normes de votre organisation.

ID du contrôle	AWS Règle de configuration	Conseils
6.4	vpc-flow-logs-enabled	Les journaux de flux VPC fournissent des informati ons détaillées sur le trafic IP circulant vers et depuis les interfaces réseau de votre réseau Amazon Virtual Private Cloud (Amazon VPC). Par défaut, le journal de flux inclut des valeurs pour les différent s composants du flux IP, y compris la source, la destinati on et le protocole.
6.5 A	guardduty-enabled-centralized	Amazon GuardDuty peut vous aider à surveiller et à détecter les événements potentiel s liés à la cybersécurité en utilisant des flux de renseigne ments sur les menaces. Il s'agit notamment de listes d'adresses IP malveillantes et de l'apprentissage automatiq ue pour identifier les activités inattendues, non autorisées et malveillantes au sein de votre environnement AWS cloud.

ID du contrôle	AWS Règle de configuration	Conseils
6.5 A	securityhub-enabled	AWS Security Hub permet de surveiller le personnel, les connexions, les appareils et les logiciels non autorisés. AWS Security Hub regroupe, organise et hiérarchise les alertes de sécurité, ou les résultats, provenant de plusieurs services. AWS Parmi ces services figurent Amazon Security Hub, Amazon Inspector, Amazon Macie, AWS Identity and Access Management (IAM) Access Analyzer et AWS Firewall Manager, ainsi que des solutions partenaires. AWS

Modèle

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour SWIFT CSP.

Bonnes pratiques de sécurité pour Amazon Elastic Container Service (Amazon ECS)

Ce pack de conformité contient des AWS Config règles basées sur Amazon ECS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon ECS.

Bonnes pratiques de sécurité pour Amazon Elastic File System (Amazon EFS)

Ce pack de conformité contient des AWS Config règles basées sur Amazon EFS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon EFS.

Bonnes pratiques de sécurité pour Amazon Elastic Kubernetes Service (Amazon EKS)

Ce pack de conformité contient des AWS Config règles basées sur Amazon EKS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon EKS.

Bonnes pratiques en matière de sécurité pour Amazon CloudFront

Ce pack de conformité contient des AWS Config règles basées sur Amazon CloudFront. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon CloudFront.

Bonnes pratiques en matière de sécurité pour Amazon OpenSearch Service

Ce pack de conformité contient des AWS Config règles basées sur Amazon OpenSearch Service. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon OpenSearch Service.

Bonnes pratiques de sécurité pour Amazon Redshift

Ce pack de conformité contient des AWS Config règles basées sur Amazon Redshift. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon Redshift.

Bonnes pratiques de sécurité pour Amazon Relational Database Service (Amazon RDS)

Ce pack de conformité contient des AWS Config règles basées sur Amazon RDS. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon RDS.

Bonnes pratiques de sécurité pour AWS Auto Scaling

Ce pack de conformité contient des AWS Config règles basées sur AWS Auto Scaling. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for AWS Auto Scaling.

Bonnes pratiques de sécurité pour AWS CloudTrail

Ce pack de conformité contient des AWS Config règles basées sur AWS CloudTrail. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for AWS CloudTrail.

Bonnes pratiques de sécurité pour AWS CodeBuild

Ce pack de conformité contient des AWS Config règles basées sur AWS CodeBuild. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for AWS CodeBuild.

Bonnes pratiques de sécurité pour Amazon ECR

Ce pack de conformité contient des AWS Config règles basées sur Amazon Elastic Container Registry (Amazon ECR). Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon ECR.

Bonnes pratiques de sécurité pour AWS Lambda

Ce pack de conformité contient des AWS Config règles basées sur AWS Lambda. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for AWS Lambda.

Bonnes pratiques de sécurité pour AWS Network Firewall

Ce pack de conformité contient des AWS Config règles basées sur AWS Network Firewall. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for AWS Network Firewall.

Bonnes pratiques en matière de sécurité pour Amazon SageMaker

Ce pack de conformité contient des AWS Config règles basées sur Amazon SageMaker. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for Amazon SageMaker.

Bonnes pratiques de sécurité pour AWS Secrets Manager

Ce pack de conformité contient des AWS Config règles basées sur AWS Secrets Manager. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for AWS Secrets Manager.

Bonnes pratiques de sécurité pour AWS WAF

Ce pack de conformité contient des AWS Config règles basées sur AWS WAF. Pour obtenir la liste de toutes les règles gérées prises en charge par AWS Config, consultez la section Liste des règles AWS Config gérées.

Consultez la `Parameters` section du modèle suivant pour connaître les noms et les descriptions des paramètres requis.

Le modèle est disponible sur GitHub : Security Best Practices for AWS WAF.

Exemples de modèle avec action de correction

Meilleures pratiques opérationnelles pour Amazon DynamoDB avec remédiation

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour Amazon DynamoDB avec remédiation.

Meilleures pratiques opérationnelles pour Amazon S3 avec correction

Le modèle est disponible sur GitHub : Meilleures pratiques opérationnelles pour Amazon S3 avec correction.

Pour plus d'informations sur la structure du modèle, voir Anatomie du modèle dans le guide de AWS CloudFormation l'utilisateur.

Packs de conformité personnalisés

Un pack de conformité personnalisé est un ensemble unique de AWS Config règles et d'actions correctives que vous pouvez déployer ensemble dans un compte et une AWS région, ou au sein d'une organisation dans. AWS Organizations

Pour créer un pack de conformité personnalisé, suivez les étapes décrites dans la section Personnalisation du modèle ci-dessous afin de créer un fichier YAML contenant la liste des Règles AWS Config gérées ou des Règles AWS Config personnalisées avec lesquelles vous souhaitez travailler.

Terminologie

AWS Config Les règles gérées sont des règles prédéfinies détenues par AWS Config.

AWS Config Les règles personnalisées sont des règles que vous créez de toutes pièces.

Il existe deux manières de créer des règles AWS Config personnalisées : avec les fonctions Lambda (Guide du AWS Lambda développeur) et avec Guard (Guard GitHub Repository), un policy-as-code langage. AWS Config les règles personnalisées créées avec AWS Lambda sont appelées règles

Lambda AWS Config personnalisées et les règles AWS Config personnalisées créées avec Guard sont appelées règles de politique AWS Config personnalisées.

Personnalisation du modèle

Création de votre fichier YAML

Pour créer un fichier YAML, ouvrez un éditeur de texte et enregistrez le fichier sous le nom .yaml.

> **Note**
>
> Votre fichier contiendra une section Paramètres et Ressources.

Paramètres

La `Parameters` section de votre fichier YAML contient les paramètres de règle de l'ensemble de AWS Config règles que vous ajouterez ultérieurement dans la `Resources` section. Créez la section `Parameters` en copiant et en collant le bloc de code suivant dans votre fichier YAML, en le personnalisant selon vos besoins et en le répétant pour chaque paramètre de règle.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

Par exemple :

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> Lorsque vous sélectionnez les AWS Config règles pour créer votre pack de conformité personnalisé, vérifiez que vous disposez des ressources fournies dans votre compte qui seront évaluées en fonction des AWS Config règles.

1. La première ligne de la section des paramètres qui suit `Parameters:` est une chaîne concaténée de *`NameOfRule`*+ Param +. *`NameOfRuleParameter`*

   a. Remplacez *`NameOfRule`* par un nom cohérent que vous avez créé pour la règle. Par exemple, cela pourrait être IamPasswordPolicypour la iam-password-policy règle.

   b. Tapez `Param`.

   c. Remplacez ensuite *`NameOfRuleParameter`* par le nom du paramètre de règle correspondant à votre règle spécifique. Pour les règles AWS Config gérées, le nom du paramètre de règle se trouve dans la liste des règles AWS Config gérées (par exemple, MinimumPasswordLengthil s'agit du nom d'un paramètre de règle pour la iam-password-policyrègle). Pour les règles AWS Config personnalisées, le nom du paramètre de règle est le nom que vous avez choisi lors de la création de la règle.

2. Si vous utilisez une règle AWS Config gérée, recherchez la AWS Config règle appropriée dans la liste des règles gérées afin de connaître les valeurs acceptées pour `Default` et `Type` pour votre règle particulière. Pour les règles AWS Config personnalisées, utilisez les valeurs que vous avez sélectionnées lors de la création de votre règle.

   > **Note**
   >
   > Pour chaque paramètre, `Type` il faut le spécifier. `Type`peut être l'une des valeurs suivantes : « String », « int », « double », « CSV », « boolean » ou « »StringMap.

Ressources

La section `Resources` répertorie les règles qui sont ajoutées à votre pack de conformité personnalisé. Ajoutez le bloc `Resources` suivant directement sous votre section `Parameters`, en le personnalisant selon vos besoins et en le répétant pour chaque règle. Pour plus d'informations sur les spécifications, consultez AWS::Config::ConfigRule.

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
```

```
        Type: AWS::Config::ConfigRule
    ...
```

Par exemple :

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> Lorsque vous sélectionnez les AWS Config règles pour créer votre pack de conformité personnalisé, vérifiez que vous disposez des ressources qui seront évaluées en fonction des AWS Config règles fournies dans votre compte. Pour plus d'informations, consultez Types de ressources pris en charge.

1. Remplacez *`NameOfRule`* par le même nom que celui que vous avez créé dans la section `Parameters`.
2. Pour les règles AWS Config gérées, remplacez *`ActualConfigRuleName`* par le titre de la page de règles appropriée dans la liste des règles AWS Config gérées. Pour les règles AWS Config personnalisées, utilisez le nom de la règle de configuration que vous avez choisi au moment de la création de la règle.
3. Remplacez *`NameOfRuleParameter`* par le même nom que celui que vous avez utilisé dans la section `Parameters`. Après les deux points, copiez et collez la même chaîne concaténée de *`NameOfRule`*+ Param + *`NameOfRuleParameter`*que celle que vous avez créée dans la section. `Parameters`
4. Remplacez *`Owner`* par la valeur appropriée.

> **Note**
>
> AWS Config Règles gérées
>
> Pour les règles AWS Config gérées, la valeur de `Owner` seraAWS.
>
> AWS Config Règles personnalisées
>
> Pour les règles AWS Config personnalisées créées avec Guard, la valeur de `Owner` seraCUSTOM_POLICY. Pour les règles AWS Config personnalisées créées avec Lambda, la valeur de `Owner` sera. CUSTOM_LAMBDA

5. Remplacez *SOURCE_IDENTIFIER* par la valeur appropriée.

> **Note**
>
> AWS Config Règles gérées
>
> Pour les règles AWS Config gérées, copiez l'identifiant en suivant le lien de la règle que vous sélectionnez dans la liste des règles AWS Config gérées (par exemple, l'identifiant source de la access-keys-rotatedrègle est ACCESS_KEYS_ROTATED).
>
> AWS Config Règles personnalisées
>
> Pour les règles AWS Config personnalisées créées avec Lambda, `SourceIdentifier` il s'agit du nom de ressource Amazon (ARN) de la AWS Lambda fonction de la règle, par exemple. `arn:aws:lambda:us-east-2:123456789012:function:`*ActualConfigRuleName* Pour les règles AWS Config personnalisées créées avec Guard, ce champ n'est pas nécessaire.

Dans l'ensemble, votre pack de conformité personnalisé rempli devrait commencer à ressembler à ce qui suit, qui est un exemple utilisant ces règles AWS Config gérées : iam-password-policy, access-keys-rotated, et iam-user-unused-credentials-check.

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
```

```
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge:
 IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

Déploiement de votre pack de conformité personnalisé

Pour déployer votre pack de conformité personnalisé, voir Déployer un pack de conformité à l'aide de la AWS Config console et le déploiement d'un pack de conformité à l'aide de l'interface de ligne de AWS Config commande.

Affichage des données de conformité dans le tableau de bord des packs de conformité

La page principale Packs de conformité affiche tous les packs de conformité actuellement disponibles dans votre Compte AWS. La page contient également le nom, l'état de déploiement et le score de conformité de chaque pack de conformité. Le score de conformité est le pourcentage du nombre de combinaisons règle-ressource conformes dans un pack de conformité par rapport au nombre total de combinaisons règles-ressources possibles dans le pack de conformité.

Vous pouvez utiliser ce tableau de bord pour déterminer le niveau de conformité de vos packs de conformité et utiliser le score de conformité pour suivre la progression des mesures correctives, effectuer des comparaisons entre différents ensembles d'exigences et évaluer l'impact d'un changement ou d'un déploiement spécifique sur un pack de conformité.

Navigation sur la page principale des packs de conformité

1. Connectez-vous à la AWS Management Console et ouvrez la console AWS Config à l'adresse https://console.aws.amazon.com/config/.
2. Accédez à la page Pack de conformité. Examinez vos packs de conformité et leurs scores de conformité. Vous pouvez également effectuer les opérations suivantes :
   - Pour ajouter et configurer un nouveau pack de conformité, choisissez Déployer le pack de conformité.
   - Pour supprimer un pack de conformité et ses données, modifier les paramètres de configuration ou consulter des détails supplémentaires, tels que l'emplacement ou les paramètres de diffusion, choisissez un pack de conformité, puis Actions.

     > **Note**
     >
     > Un pack de conformité déployé ne peut pas être modifié. Vous pouvez modifier les autres sélections à tout moment en choisissant le nom du pack de conformité et en sélectionnant Modifier dans le menu déroulant Actions.

   - Pour consulter l'historique des changements d'état de conformité, choisissez un pack de conformité, puis Chronologie du pack de conformité. Pour plus d'informations, consultez Affichage de la chronologie de l'historique de conformité des packs de conformité.

- Pour afficher l'état du déploiement, le score de conformité, la chronologie des scores de conformité et les règles d'un pack de conformité dans une vue détaillée, choisissez un pack de conformité, puis Afficher.

En savoir plus

Conditions préalables du pack de conformité

Exemples de modèles de pack de conformité

Déploiement d'un pack de conformité

Limites de service AWS

Affichage de la chronologie de l'historique de conformité des packs de conformité

AWS Config prend en charge le stockage des modifications de l'état de conformité de vos packs de conformité. Vous pouvez ainsi consulter l'historique des changements d'état de conformité. Ces changements d'état de conformité sont présentés sous forme de chronologie. Cette chronologie capture les changements sous forme d'éléments `ConfigurationItems` sur une période de temps. Vous pouvez également utiliser cette fonctionnalité pour rechercher des règles spécifiques non conformes dans un pack de conformité.

Vous pouvez accepter ou refuser l'enregistrement de tous les types de ressources dans AWS Config. Si vous avez choisi d'enregistrer tous les types de ressources, commence AWS Config automatiquement à enregistrer l'historique de conformité du pack de conformité tel qu'évalué par AWS Config Rules. Par défaut, AWS Config enregistre les modifications de configuration pour toutes les ressources prises en charge. Vous pouvez également sélectionner uniquement le type de ressource spécifique de l'historique de conformité du pack de conformité : `AWS::Config::ConformancePackCompliance`. L'enregistrement du type de ressource `AWS::Config::ConformancePackCompliance` est disponible sans frais supplémentaires. Pour plus d'informations, voir Sélection des AWS Config enregistrements de ressources.

Un pack de conformité est conforme si toutes les règles qui lui sont appliquées sont conformes. Il est non conforme si l'une des règles est non conforme. L'état de conformité d'un pack de conformité est INSUFFICIENT_DATA uniquement si toutes les règles qui lui sont appliquées ne peuvent pas

être évaluées en raison de données insuffisantes. Si certaines règles d'un pack de conformité sont conformes alors que l'état de conformité des autres règles de ce même pack de conformité est INSUFFICIENT_DATA, le pack de conformité est conforme. La conformité d'un pack de conformité n'est pas évaluée en une seule fois. L'évaluation de certaines règles peut prendre plus de temps que celle d'autres règles. La conformité est évaluée pour des groupes de règles en même temps et continue par étapes jusqu'à ce que toutes les règles d'un pack de conformité aient été évaluées.

Rubriques

- Affichage de la chronologie de conformité
- Interrogation de l'historique de conformité

Affichage de la chronologie de conformité

Accédez à la chronologie de conformité en sélectionnant un pack de conformité spécifique sur la page principale Pack de conformité.

1. Accédez à la page Pack de conformité.
2. Sur la page principale Pack de conformité, choisissez un pack de conformité spécifique, puis Chronologie du pack de conformité.

> **Note**
>
> Vous pouvez également utiliser la chronologie de conformité figurant sur la page des détails du pack de conformité. Choisissez un pack de conformité, puis l'option Afficher les détails dans le menu déroulant Actions. Sur cette page, choisissez Chronologie du pack de conformité.

La chronologie présente l'historique des changements d'état de conformité d'un pack de conformité. Vous pouvez effectuer les actions suivantes :

1. Développez une modification de conformité pour afficher l'état de line-by-line conformité de chaque règle d'un pack de conformité.
2. Dans la vue agrandie, choisissez une règle spécifique pour afficher la page contenant ses détails.

Interrogation de l'historique de conformité

Interrogez l'historique de conformité à get-resource-config-history l'aide du type de ressource`AWS::Config::ConformancePackCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

Vous devez voir des résultats similaires à ce qui suit :

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
```

```
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

Pour plus d'informations, consultez Supported Resource Types (AWS Config) et GetResourceConfigHistorydans la référence de l'API.

Déploiement d'un pack de conformité à l'aide de la console AWS Config

Dans la page Conformance packs (Packs de conformité), vous pouvez déployer un pack de conformité pour un compte dans une région. Vous pouvez également modifier et supprimer le pack de conformité déployé.

Déploiement d'un pack de conformité à l'aide de modèles

Vous pouvez déployer un pack de conformité à l'aide d'AWS Configexemples de modèles ou de votre propre modèle personnalisé. Pour obtenir des instructions sur la façon de créer des packs de conformité personnalisés, voir Pack de conformité personnalisé.

1. Connectez-vous à la AWS Management Console et ouvrez la console AWS Config à l'adresse https://console.aws.amazon.com/config/.
2. Accédez à la page Conformance packs (Packs de conformité) et choisissez Deploy conformance pack (Déployer le pack de conformité).
3. Dans la page Specify template (Spécifier un modèle), choisissez un modèle ou utilisez un modèle existant. Pour plus d'informations, consultez Exemples de Pack de conformité.

   - Si vous choisissez Utiliser un exemple de modèle, sélectionnez un modèle d'exemple dans la liste déroulante des exemples de modèles.

     Pour obtenir des informations sur le contenu de chaque modèle, veuillez consulter Exemples de modèles de pack de conformité.
   - Si vous choisissez Template is ready (Le modèle est prêt), spécifiez la source du modèle. Il s'agit d'un URI Amazon S3, d'un AWS Systems Manager document (document SSM) ou d'un modèle que vous chargez.

     Si votre modèle est supérieur à 50 Ko, chargez-le dans le compartiment S3 et sélectionnez l'emplacement de ce compartiment S3. Par exemple : s3://*bucketname/prefix*.

     > **Important**
     >
     > Choose Template is ready si vous avez créé votre fichier YAML de pack de conformité à partir de zéro sur la base d'un pack de conformité personnalisé.
4. Choisissez Suivant.
5. Sur la page Specify conformance pack details (Spécifier les détails du pack de conformité), saisissez le nom de votre pack de conformité.

   Le nom du pack de conformité doit être un nom unique comportant au maximum 256 caractères alphanumériques. Le nom peut contenir des traits d'union mais ne peut pas contenir d'espaces.
6. Facultatif : ajoutez un paramètre.

Les paramètres sont définis dans votre modèle et vous aident à gérer et organiser vos ressources.

7. Choisissez Suivant.
8. Dans la page Review and deploy (Vérifier et déployer), passez en revue l'ensemble des informations.

   Vous pouvez modifier les détails du modèle et les détails du pack de conformité en choisissant Edit (Modifier).
9. Choisissez Deploy conformance pack (Déployer le pack de conformité).

   AWS Config affiche le pack de conformité dans la page du pack de conformité avec le statut approprié.

   Si votre déploiement de pack de conformité échoue, vérifiez vos autorisations, vérifiez que vous avez effectué les étapes prérequises et réessayez. Ou vous pouvez contacterAWS Support.

Pour déployer un pack de conformité à l'aide d'un exemple de modèle avec des corrections, consultez Conditions préalables à l'utilisation d'un pack de conformité avec la correction, puis utilisez la procédure précédente.

Pour déployer un pack de conformité avec une ou plusieurs règles AWS Config, reportez-vous à Conditions préalables à l'utilisation d'un pack de conformité avec une ou plusieurs règles AWS Config.

Modifier un pack de conformité

1. Pour modifier un pack de conformité, sélectionnez le pack souhaité dans le tableau.
2. Choisissez Actions, puis Edit (Modifier).
3. Sur la page Edit conformance pack (Modifier le pack de conformité) vous pouvez modifier les détails du modèle, l'exemple de modèle, le pack de conformité et les paramètres.

   Vous ne pouvez pas modifier le nom du pack de conformité.
4. Choisissez Save Changes (Enregistrer les modifications).

   Le pack de conformité est affiché avec les règles AWS Config.

Supprimer un pack de conformité

1. Pour supprimer un pack de conformité, sélectionnez le pack souhaité dans le tableau.
2. Choisissez Actions, puis Delete (Supprimer).
3. Dans la boîte de dialogue *`Delete conformance pack (Supprimer le pack de conformité)`*, confirmez si vous souhaitez supprimer définitivement ce pack de conformité.

   > **Important**
   >
   > Vous ne pouvez pas annuler cette action. Lorsque vous supprimez un pack de conformité, vous supprimez toutes les règles AWS Config et actions de correction figurant dans le pack de conformité.

4. Entrez Delete (Supprimer) et choisissez Delete (Supprimer).

   Dans la page Conformance packs (Packs de conformité), vous pouvez voir le statut du déploiement, tel que Deleting (En cours de suppression), jusqu'à ce que le pack de conformité soit entièrement supprimé.

Déploiement d'un pack de conformité à l'aide de l' AWS Command Line Interface

Vous pouvez déployer, afficher, mettre à jour, consulter l'état de conformité et supprimer un pack de AWS Config conformité à l'aide du AWS Command Line Interface (AWS CLI).

AWS CLI Il s'agit d'un outil unifié pour gérer vos AWS services. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs AWS services depuis la ligne de commande et utiliser des scripts pour les automatiser. Pour plus d'informations sur les AWS CLI outils AWS CLI et pour obtenir des instructions sur leur installation, reportez-vous à ce qui suit dans le guide de AWS Command Line Interface l'utilisateur.

- AWS Command Line Interface Guide de l'utilisateur
- Préparation de l’installation de l’ AWS Command Line Interface

Si nécessaire, saisissez `aws configure` pour configurer le AWS CLI afin d'utiliser une AWS région dans laquelle des packs de conformité sont disponibles.

Rubriques

- Déployer un pack de conformité
- Afficher un pack de conformité
- Afficher l'état du pack de conformité
- Afficher l'état de conformité du pack de conformité
- Obtenir les détails de conformité pour un pack de conformité spécifique
- Supprimer un pack de conformité

Déployer un pack de conformité

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez l'une des commandes suivantes pour déployer un pack de conformité nommé **`MyConformancePack`**. La source du modèle est soit un URI Amazon S3, soit un modèle que vous chargez, soit un AWS Systems Manager document (document SSM).

   URI Amazon S3

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://AmazonS3BucketName/templateName.yaml"
   --delivery-s3-bucket AmazonS3BucketName
   ```

   Modèle YAML de votre répertoire local

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager Document (Document Systems Manager)

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket AmazonS3BucketName
   ```

3. Appuyez sur Entrée pour exécuter la commande.

Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Pour plus d'informations sur la création d'un modèle YAML pour un pack de conformité, consultez Pack de conformité personnalisé.

Afficher un pack de conformité

1. Entrez la commande suivante.

```
aws configservice describe-conformance-packs
```

OU

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Afficher l'état du pack de conformité

1. Entrez la commande suivante.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Afficher l'état de conformité du pack de conformité

1. Entrez la commande suivante.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
```

```
        }
    ]
}
```

Obtenir les détails de conformité pour un pack de conformité spécifique

1. Entrez la commande suivante.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. Vous devez visualiser des résultats similaires à ce qui suit.

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
```

```
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

Supprimer un pack de conformité

Entrez la commande suivante.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

En cas de réussite, la commande s'exécute sans sortie supplémentaire.

> **Important**
>
> Vous ne pouvez pas annuler cette action. Lorsque vous supprimez un pack de conformité, vous supprimez toutes les AWS Config règles et actions correctives qu'il contient.

Gestion des packs de conformité (API)

Utilisez les actions AWS Config d'API suivantes pour gérer les packs de conformité :

- DeleteConformancePack, supprime le pack de conformité spécifié ainsi que toutes les AWS Config règles et tous les résultats d'évaluation contenus dans ce pack de conformité.
- DescribeConformancePackCompliance, renvoie les informations de conformité pour chaque règle de ce pack de conformité.
- DescribeConformanceRegroupe, renvoie une liste d'un ou de plusieurs packs de conformité.
- DescribeConformancePackStatus, fournit l'état de déploiement d'un ou de plusieurs packs de conformité.
- GetConformancePackComplianceDétails : renvoie les informations de conformité d'un pack de conformité pour toutes les AWS ressources surveillées par le pack de conformité.
- GetConformancePackComplianceRésumé, renvoie les informations de conformité pour le pack de conformité en fonction des résultats de conformité cumulés de toutes les règles de ce pack de conformité.

- ListConformancePackComplianceScores, renvoie une liste des scores de conformité des packs de conformité.
- PutConformanceEmballer, créer ou mettre à jour un pack de conformité.

Gestion des packs de conformité dans tous les comptes de votre organisation

AWS Config À utiliser pour gérer les packs de conformité dans l'ensemble Comptes AWS d'une organisation. Vous pouvez effectuer les actions suivantes :

- Déployez, mettez à jour et supprimez de manière centralisée les packs de conformité dans l'ensemble des comptes membres d'une organisation dans AWS Organizations.
- Déployez un ensemble commun de AWS Config règles et d'actions correctives pour tous les comptes et spécifiez les comptes pour lesquels les AWS Config règles et les actions correctives ne doivent pas être créées.
- Utilisez le compte de gestion AWS Organizations pour appliquer la gouvernance en vous assurant que les AWS Config règles sous-jacentes et les mesures correctives ne sont pas modifiables par les comptes membres de votre organisation.

Considérations

Pour les déploiements dans différentes régions

L'appel d'API pour déployer des règles et des packs de conformité entre les comptes est spécifique à AWS la région. Au niveau de l'organisation, vous devez modifier le contexte de votre appel d'API vers une autre région si vous souhaitez déployer des règles dans d'autres régions. Par exemple, pour déployer une règle dans la région USA Est (Virginie du Nord), remplacez la région par USA Est (Virginie du Nord), puis appelez `PutOrganizationConfigRule`.

Pour les comptes au sein d'une organisation

Si un nouveau compte rejoint une organisation, la règle ou le pack de conformité est déployé(e) sur ce compte. Lorsqu'un compte quitte une organisation, la règle ou le pack de conformité est supprimé(e).

Si vous déployez une règle organisationnelle ou un pack de conformité dans un compte administrateur d'organisation avant d'établir un administrateur délégué et de déployer une règle

organisationnelle ou un pack de conformité dans le compte administrateur délégué, vous ne pourrez pas voir la règle organisationnelle ou le pack de conformité dans le compte administrateur de l'organisation depuis le compte administrateur délégué, ni voir la règle organisationnelle ou le pack de conformité dans le compte administrateur délégué depuis le compte administrateur de l'organisation. Les DescribeOrganizationConformancePacksAPI DescribeOrganizationConfigRuleset peuvent uniquement voir et interagir avec les ressources liées à l'organisation qui ont été déployées depuis le compte appelant ces API.

Mécanisme de nouvelle tentative pour les nouveaux comptes ajoutés à une organisation

Le déploiement des règles organisationnelles et des packs de conformité existants fera l'objet d'une nouvelle tentative uniquement dans les 7 heures suivant l'ajout d'un compte à votre organisation si aucun enregistreur n'est disponible. Vous devez créer un enregistreur s'il n'en existe pas dans les 7 heures qui suivent l'ajout d'un compte à votre organisation.

Comptes de gestion de l'organisation, administrateurs délégués et rôles liés aux services

Si vous utilisez un compte de gestion d'organisation et que vous avez l'intention de faire appel à un administrateur délégué pour le déploiement organisationnel, sachez que cela AWS Config ne créera pas automatiquement le rôle lié au service (SLR). Vous devez créer manuellement le rôle lié au service (SLR) séparément à l'aide d'IAM.

Si vous ne possédez pas de SLR pour votre compte de gestion, vous ne pourrez pas déployer de ressources vers ce compte à partir d'un compte d'administrateur délégué. Vous pourrez toujours déployer des packs de conformité sur les comptes membres à partir de comptes de gestion et d'administrateur délégué. Pour plus d'informations, consultez la section Utilisation des rôles liés à un service dans le Guide de l'AWS Identity and Access Management utilisateur (IAM).

Déploiement

To deploy with the AWS Management Console

Pour déployer un pack de conformité au sein d'une organisation à partir de la AWS console, utilisez AWS Systems Manager. Pour plus d'informations, consultez la section Déployer des packs de AWS Config conformité dans le guide de AWS Systems Manager l'utilisateur.

To deploy with the AWS API

Pour plus d'informations sur la manière AWS Config d'intégrer AWS Organizations, consultez AWS Config et AWS Organizations dans le Guide de AWS Organizations l'utilisateur. Assurez-

vous que AWS Config l'enregistrement est activé avant d'utiliser les API suivantes pour gérer les règles des packs de conformité Comptes AWS dans l'ensemble d'une organisation :

- DeleteOrganizationConformancePack, supprime le pack de conformité d'organisation spécifié ainsi que toutes les règles de configuration et les actions de correction de tous les comptes membres de cette organisation.
- DescribeOrganizationConformancePacks, renvoie une liste des packs de conformité de l'organisation.
- DescribeOrganizationConformancePackStatuts : indique l'état du déploiement du pack de conformité d'une organisation.
- GetOrganizationConformancePackDetailedStatus, renvoie le statut détaillé de chaque compte membre au sein d'une organisation pour un pack de conformité d'organisation donné.
- PutOrganizationConformancePack, déploie des packs de conformité sur les comptes des membres d'une AWS organisation.

Prise en charge de la région

Le déploiement de packs de conformité sur les comptes membres d'une AWS organisation est pris en charge dans les régions suivantes.

Nom de la région	Région	Point de terminaison	Protocole
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Résolution des problèmes

État d'échec d'un pack de conformité

Si une erreur s'affiche indiquant que le pack de conformité a échoué lors de sa création, de sa mise à jour ou de sa suppression, vous pouvez vérifier le statut de votre pack de conformité.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

Vous devez visualiser des résultats similaires à ce qui suit.

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

Consultez le ConformancePackStatusReasonpour obtenir des informations sur l'échec.

Lorsque stackArn est présent dans la réponse

Si le message d'erreur n'est pas clair ou si l'échec est dû à une erreur interne, accédez à la console AWS CloudFormation et procédez comme suit :

1. Recherchez stackArn à partir de la sortie.
2. Choisissez l'onglet Événements de la CloudFormation pile et recherchez les événements ayant échoué.

   Le motif du statut indique pourquoi le pack de conformité a échoué.

Lorsque stackArn n'est pas présent dans la réponse

Si vous recevez un échec lors de la création d'un pack de conformité mais que le StackArn n'est pas présent dans la réponse d'état, cela peut être dû au fait que la création de la pile a échoué, puis a été CloudFormation annulée et supprimée. Accédez à la CloudFormation console et recherchez les piles dont l'état est supprimé. La pile qui a échoué peut y être disponible. La CloudFormation pile contient le nom du pack de conformité. Si vous trouvez la pile défaillante, cliquez sur l'onglet Événements de la CloudFormation pile et recherchez les événements ayant échoué.

Si aucune de ces étapes n'a fonctionné et si la cause de l'échec est une erreur de service interne, réessayez ou contactez le AWS Support Centre.

Des règles en suspens dans un pack de conformité

Le déploiement d'un pack de conformité implique la création d'une AWS CloudFormation pile sous-jacente en arrière-plan pour déployer les règles du modèle de pack de conformité. Ces règles sont liées à un service et ne peuvent être ni mises à jour ni supprimées en dehors du pack de conformité.

Si vous apportez des modifications à la CloudFormation pile sous-jacente, le pack de conformité et ses règles deviennent ingérables. Ces règles ingérables sont des règles suspendues.

Dérive entre la CloudFormation pile et le pack de conformité

Vous pouvez mettre à jour les noms des règles dans un modèle de pack de conformité directement depuis la CloudFormation console. Si vous mettez à jour le modèle directement depuis la CloudFormation console, cela ne met pas à jour le pack de conformité déployé.

Cette dérive crée une règle pendante. Si vous essayez de supprimer la règle du pack de conformité, vous recevez un message d'erreur similaire au suivant :

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

Si vous essayez de supprimer le pack de conformité, la règle suspendue ne peut pas être supprimée et vous recevez un message d'erreur similaire au suivant :

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

Pour résoudre ce problème, procédez comme suit :

1. Supprimer la pile. Pour plus d'informations, consultez la section Suppression d'une pile sur la AWS CloudFormation console dans le Guide de CloudFormation l'utilisateur.
2. Supprimez le pack de conformité à l'aide de la AWS Config console ou de l'API DeleteConformancePack. S'il s'agit d'un pack de conformité organisationnel et que vous utilisez le compte de gestion ou d'administrateur délégué, utilisez l'DeleteOrganizationConformancePackAPI.

3. Contactez le AWS Support Centre en indiquant le nom de ressource Amazon (ARN) correspondant aux règles en suspens dans le pack de conformité pour vous aider à nettoyer votre compte.

Pour éviter ce problème, n'oubliez pas les bonnes pratiques suivantes :

- N'apportez jamais de mise à jour directe à la CloudFormation pile d'un pack de conformité.
- N'essayez jamais d'apporter des modifications susceptibles de créer une dérive entre le pack de conformité et sa CloudFormation pile sous-jacente.
- Le rôle lié au service (SLR) pour les packs de conformité ne peut pas être modifié. Assurez-vous que les ressources que vous mettez à jour font partie de la politique d'autorisation du SLR.

CloudFormation Pile supprimée pour un pack de conformité

Sauf en cas de dérive entre la CloudFormation pile et le pack de conformité, il n'est jamais recommandé de supprimer les règles d'un pack de conformité ou de sa CloudFormation pile directement depuis la CloudFormation console.

Pour résoudre ce problème, contactez le AWS Support Centre en indiquant le nom de ressource Amazon (ARN) correspondant aux règles en suspens dans le pack de conformité afin de vous aider à nettoyer votre compte.

Pour éviter ce problème, n'oubliez pas les bonnes pratiques suivantes :

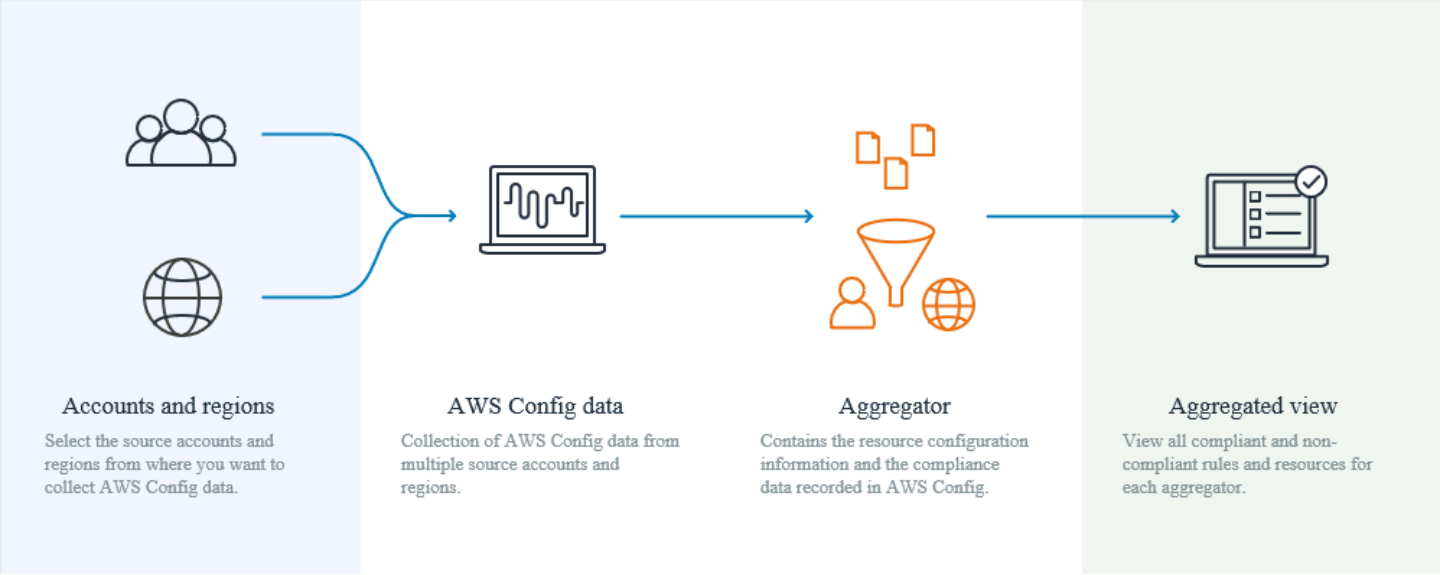
- Ne supprimez jamais la CloudFormation pile sous-jacente d'un pack de conformité.
- Supprimez les packs de conformité à l'aide de l'API DeleteConformancePack. S'il s'agit d'un pack de conformité organisationnel et que vous utilisez le compte de gestion ou d'administrateur délégué, utilisez l'DeleteOrganizationConformancePackAPI.

Regroupement des données de plusieurs comptes et plusieurs régions

Un agrégateur est un type de AWS Config ressource qui collecte des données AWS Config de configuration et de conformité à partir des éléments suivants :

- Plusieurs comptes et plusieurs AWS régions.
- Un seul compte et plusieurs AWS régions.
- Une organisation AWS Organizations et tous les comptes de cette organisation qui ont été AWS Config activés.

Utilisez un agrégateur pour afficher la configuration des ressources et les données de conformité enregistrées dans AWS Config. Un agrégateur utilise un compartiment Amazon S3 pour stocker des données agrégées. Il récupère régulièrement des instantanés de configuration à partir des comptes sources et les stocke dans le compartiment S3 désigné. L'image suivante montre comment un agrégateur collecte les AWS Config données de plusieurs comptes et régions.



Cas d'utilisation

- Surveillance de la conformité : vous pouvez agréger les données de conformité pour évaluer le niveau de conformité global de votre organisation, ou entre les comptes et les régions.

- Suivi des modifications : vous pouvez suivre les modifications apportées aux ressources au fil du temps au sein de votre organisation, ou entre les comptes et les régions.
- Relations entre les ressources : vous pouvez analyser les dépendances et les relations entre les ressources au sein de votre organisation, ou entre les comptes et les régions.

> **Note**
>
> Les agrégateurs fournissent une vue en lecture seule des comptes source et des régions que l'agrégateur est autorisé à consulter en répliquant les données des comptes sources vers le compte agrégateur. Les agrégateurs ne fournissent pas d'accès mutant à un compte ou à une région source. Par exemple, cela signifie que vous ne pouvez pas déployer de règles via un agrégateur ou transférer des fichiers instantanés vers un compte ou une région source via un agrégateur.
> L'utilisation d'agrégateurs n'entraîne aucun coût supplémentaire.

Terminologie

Un compte source est le compte Compte AWS à partir duquel vous souhaitez agréger les données de configuration et de conformité des AWS Config ressources. Un compte source peut être un compte individuel ou une organisation dans AWS Organizations. Vous pouvez fournir des comptes sources individuellement ou vous pouvez les récupérer via AWS Organizations.

Une région source est la AWS région à partir de laquelle vous souhaitez agréger les données AWS Config de configuration et de conformité.

Un compte agrégateur est un compte dans lequel vous créez un agrégateur.

L'autorisation fait référence aux autorisations que vous accordez à un compte agrégateur et à une région pour collecter vos données AWS Config de configuration et de conformité. Aucune autorisation n'est requise si vous regroupez des comptes source qui font partie de AWS Organizations.

Comment agréger les données

Pour agréger vos AWS Config données provenant de comptes sources et de régions, commencez par :

1. Ajout d'un agrégateur pour agréger les données AWS Config de configuration et de conformité provenant de plusieurs comptes et régions. Pour plus d'informations, consultez Configuration d'un agrégateur à l'aide de la console et Configuration d'un agrégateur à l'aide du AWS Command Line Interface.
2. Autoriser les comptes agrégateurs à collecter des données de AWS Config configuration et de conformité. Pour plus d'informations, consultez Autoriser les comptes agrégateurs à collecter des données de AWS Config configuration et de conformité à l'aide de la console et Autoriser les comptes agrégateurs à collecter des données de AWS Config configuration et de conformité à l'aide du AWS Command Line Interface.

> **Note**
>
> Il existe deux types d'agrégateurs : l'agrégateur de comptes individuels et l'agrégateur Organization
>
> Pour l'agrégateur de comptes individuels, une autorisation est requise pour toutes les régions de compte source incluses, y compris les régions de compte externe ou les régions de compte membre de l'organisation.
>
> Pour l'agrégateur d'organisations, aucune autorisation n'est requise pour les régions du compte membre de l'organisation, car l'autorisation est intégrée au service Organizations.

3. Surveillance des données de conformité pour les règles et les comptes dans la vue agrégée. Pour plus d'informations, consultez Affichage des données de conformité et d'inventaire dans le tableau de bord Agrégateur.

Prise en charge de la région

Actuellement, l'agrégation de données multicomptes et multirégions est prise en charge dans les régions suivantes :

Nom de la région	Région	Point de terminaison	Protocole	
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS	

Nom de la région	Région	Point de terminaison	Protocole
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Afrique (Le Cap)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asie-Pacifique (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada Ouest (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europe (Espagne)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israël (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Moyen-Orient (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Dépannage pour le regroupement des données de plusieurs comptes et plusieurs régions

AWS Config peut ne pas agréger les données des comptes sources pour l'une des raisons suivantes :

Si cela se produit	Faites ceci
AWS Config n'est pas activé dans le compte source pour les comptes d'une organisation.	Activez AWS Config dans le compte source et autorisez le compte agrégateur à collecter des données.
L'autorisation n'est pas accordée à un compte Aggregator.	Connectez-vous au compte source et autorisez le compte agrégateur à collecter des AWS Config données.

Si cela se produit	Faites ceci
Il s'est peut-être produit un problème temporaire qui empêche le regroupem ent des données.	le regroupement de données est sujet à des retards. Patientez quelques minutes.

AWS Config peut ne pas agréger les données d'une organisation pour l'une des raisons suivantes :

Si cela se produit	Faites ceci
AWS Config ne peut pas accéder aux informations de votre organisation en raison d'un rôle IAM non valide.	Créez un rôle IAM ou sélectionnez un rôle IAM valide dans la liste des rôles IAM. **Note** Si le rôle IAM n'est pas valide pendant plus de 24 heures, les données sont AWS Config supprimées pour l'ensemble de l'organisation.
AWS Config l'accès au service est désactivé dans votre organisation.	Vous pouvez activer l'intégration entre AWS Config et AWS Organizations via l'`EnableAWSServiceAccess` API. Si vous choisissez Ajouter mon organisation dans la console, l'intégration entre AWS Config et est AWS Config automatiquement activée AWS Organizations.
AWS Config ne peut pas accéder aux informations de votre organisation car toutes les fonctionnalités ne sont pas activées dans votre organisation.	Activez toutes les fonctionnalités de AWS Organizations la console.
Les changements organisationnels tels que l'ajout d'un compte, la suppression d'un compte, ainsi que l'activation et la désactivation de l'accès aux services ne sont pas immédiatement mis à jour	L’application des changements organisationnels nécessite un délai de 2 heures. Patientez 2 heures pour observer l’application de tous les changements au sein de l'organisation.

Si cela se produit	Faites ceci
dans les régions du Moyen-Orient (Bahreïn) et de l'Asie-Pacifique (Hong Kong).	

Affichage des données de conformité et d'inventaire dans le tableau de bord Agrégateur

Le tableau de bord de la page Agrégateurs affiche les données de configuration de vos AWS ressources agrégées. Il fournit une vue d'ensemble de vos règles, de vos packs de conformité et de leurs états de conformité.

Le tableau de bord fournit le nombre total de AWS ressources. Les types de ressources et les comptes source sont classés en fonction du plus grand nombre de ressources. Il indique également le nombre de règles conformes et non conformes, ainsi que celui des packs de conformité. Les règles non conformes sont classées en fonction du plus grand nombre de ressources non conformes. Les packs de conformité et les comptes sources non conformes sont classés selon le plus grand nombre de règles non conformes.

Après la configuration AWS Config, il commence à agréger les données des comptes sources spécifiés dans un agrégateur. L’affichage de l'état de conformité des règles peut prendre quelques minutes.

Utilisation du tableau de bord Agrégateur

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Accédez à la page Agrégateurs. Vous pouvez consulter :
   - Vos règles et leurs états de conformité.
   - Vos packs de conformité et leurs états de conformité.
   - Vos AWS ressources et leurs données de configuration.
3. Choisissez un agrégateur dans le tableau de bord. Filtrez vos agrégateurs en fonction de leur nom. Vous pouvez afficher les widgets suivants :
   - Inventaire des ressources

Affichez les 10 principaux types de ressources dans l'agrégateur sélectionné, par ordre décroissant en fonction du nombre de ressources. Choisissez le nombre total de ressources pour l'agrégateur sélectionné, affiché entre parenthèses après Inventaire des ressources, pour accéder à la page Ressources agrégée, où vous pouvez afficher toutes les ressources d'un agrégateur. Vous pouvez également choisir un type de ressource dans le widget pour accéder à la page Ressources agrégée, filtrée en fonction du type de ressource spécifié.

- Comptes en fonction du nombre de ressources

  Affichez les cinq principaux comptes dans l'agrégateur sélectionné, par ordre décroissant en fonction du nombre de ressources. Choisissez un compte dans le widget pour accéder à la page Ressources, filtrée en fonction du compte spécifié.

- Règles non conformes

  Affichez les cinq principales règles non conformes dans l’agrégateur sélectionné, par ordre décroissant, en fonction du nombre de ressources non conformes. Choisissez une règle dans le widget pour accéder à la page des détails de la règle spécifiée. Choisissez Afficher toutes les règles non conformes pour accéder à la page Règles agrégée, où vous pouvez consulter toutes les règles d'un agrégateur.

- Comptes en fonction des règles non conformes

  Affichez les cinq principaux comptes dans l’agrégateur sélectionné, par ordre décroissant, en fonction du nombre de ressources non conformes. Choisissez un compte dans le widget pour accéder à la page Règles agrégée, où vous pouvez consulter toutes les règles d'un agrégateur filtré en fonction du compte spécifié.

- Comptes en fonction des packs de conformité non conformes

  Affichez les cinq principaux comptes dans l’agrégateur sélectionné, par ordre décroissant, en fonction du nombre de packs de conformité non conformes. Choisissez un compte dans le widget pour accéder à la page Packs de conformité agrégée, où vous pouvez consulter tous les packs de conformité d’un agrégateur filtré en fonction du compte spécifié.

4. Dans le panneau de navigation sur la gauche, choisissez l'une des options suivantes dans le menu déroulant :

   - Tableau de bord de conformité

     Consultez des tableaux de bord de conformité automatisés à l'aide des widgets qui résument les informations relatives à la conformité des ressources au sein de votre agrégateur. Vous

pouvez consulter des données, notamment les 10 principaux types de ressources en fonction des ressources non conformes, ainsi que les 10 principaux packs de conformité au niveau des comptes selon les règles non conformes. Pour en savoir plus sur ces graphiques et tableaux, consultez Tableaux de bord de conformité.

- Packs de conformité

  Consultez tous les packs de conformité créés et liés aux différents packs au Comptes AWS sein de votre agrégateur. La page Pack de conformité affiche un tableau répertoriant le nom, la région, l'ID de compte et l'état de conformité de chaque pack de conformité. Sur cette page, vous pouvez choisir un pack de conformité et sélectionner l'option Afficher les détails pour en savoir plus sur ses règles et ses ressources, ainsi que sur leur état de conformité.

- Règles

  Consultez toutes les règles qui sont créées et liées aux différents comptes AWS de votre agrégateur. La page Règle affiche un tableau répertoriant le nom, l'état de conformité, la région et le compte de chaque règle. Sur cette page, vous pouvez choisir une règle et l'option Afficher les détails pour obtenir des informations, telles que son agrégateur, sa région, son ID de compte et les ressources concernées.

- Tableau de bord d'inventaire

  Consultez des tableaux de bord d'inventaire automatisés à l'aide des widgets qui résument les informations relatives aux données de configuration des ressources au sein de votre agrégateur. Vous pouvez consulter des données telles que les 10 principaux types de ressources en fonction du nombre de ressources et les 10 principaux comptes en fonction du nombre de ressources. Pour en savoir plus sur ces graphiques et tableaux, consultez Tableaux de bord d'inventaire.

- Ressources

  Consultez toutes les ressources qui sont enregistrées et liées aux différents comptes AWS de votre agrégateur. Sur la page Ressource, choisissez une ressource et sélectionnez l'option Afficher les détails pour afficher ses détails, les règles qui lui sont associées et la configuration actuelle des ressources. Vous pouvez également consulter des informations sur la ressource, notamment son agrégateur, sa région, son ID de compte, son nom, son type de ressource et son ID de ressource.

- Autorisations

Consultez et gérez tous les comptes actuellement autorisés ou en attente d'autorisation. Sur la page Autorisations, choisissez Ajouter une autorisation pour accorder un accès à un autre compte. Sélectionnez Supprimer une autorisation pour révoquer l'accès depuis un ID de compte.

> **Note**
>
> Dépannage
>
> Le message La collecte de données de l'ensemble des comptes et régions sources est incomplète s'affiche dans la vue agrégée pour les raisons suivantes :
>
> - Le transfert des AWS Config règles non conformes et des données de configuration des AWS ressources est en cours.
> - AWS Config Impossible de trouver les règles correspondant au filtre que vous avez appliqué. Sélectionnez le compte ou la région appropriés et réessayez.
>
> Le message La collecte de données de votre organisation est incomplète. est susceptible de s'afficher dans la vue agrégée. Vous pouvez afficher les données ci-dessous uniquement pendant 24 heures. Ce message s'affiche pour les raisons suivantes :
>
> - AWS Config Impossible d'accéder aux informations de votre organisation en raison d'un rôle IAM non valide. Si le rôle IAM n'est pas valide pendant plus de 24 heures, AWS Config supprime les données de l'ensemble de l'organisation.
> - AWS Config l'accès au service est désactivé dans votre organisation.

Tableau de bord de conformité

Consultez des tableaux de bord de conformité automatisés à l'aide des widgets qui résument les informations relatives à la conformité des ressources au sein de votre agrégateur. Ce tableau de bord affiche uniquement les règles associées à des résultats de conformité.

> **Note**
>
> Limites

Les informations contenues dans le tableau de bord de conformité sont fournies par la fonctionnalité de requêtes avancées de AWS Config, et cette fonctionnalité ne prend pas en charge les structures imbriquées ni le déballage de tableaux imbriqués. Cela signifie que le tableau de bord de conformité affiche la conformité globale d'une ressource et non l'état de conformité de chaque règle spécifique qui rend compte d'une ressource.
Par exemple, si vous cochez l'élément de configuration (CI) pour le type de ressource`AWS::Config::ResourceCompliance`, le tableau de bord affichera les résultats de conformité pour toutes les règles relatives à cette ressource. Si 10 règles font état de la ressource, que 9 d'entre elles sont CONFORMES et qu'une seule est NON CONFORME, la conformité globale de cette ressource sera NON CONFORME.

Résumé de la conformité en fonction des ressources

Affiche un graphique circulaire comparant le nombre de ressources conformes aux ressources non conformes de l'agrégateur sélectionné. Passez la souris sur le graphique pour voir le nombre et le pourcentage exacts de ressources conformes et non conformes.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Les 10 principaux types de ressources selon les ressources non conformes

Affiche un graphique à barres horizontales comparant jusqu'à 10 types de ressources provenant de l'agrégateur sélectionné par ordre décroissant du nombre de ressources non conformes. Passez la souris sur le graphique pour voir le nombre exact de ressources non conformes pour chaque type de ressource.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Les 10 comptes les plus utilisés en termes de ressources non conformes

Les 10 principaux comptes selon les ressources non conformes affichent un graphique à barres horizontales comparant jusqu'à 10 comptes de l'agrégateur sélectionné par ordre décroissant en fonction du nombre de ressources non conformes. Passez la souris sur le graphique pour voir le nombre exact de ressources non conformes pour chaque compte.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Les 10 principales régions en termes de ressources non conformes

Affiche un graphique à barres horizontales comparant jusqu'à 10 régions dans lesquelles l'agrégateur sélectionné collecte des données par ordre décroissant en fonction du nombre de ressources non conformes. Passez la souris sur le graphique pour voir le nombre exact de ressources non conformes pour chaque région.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné.

Les 10 meilleurs packs de conformité au niveau des comptes selon les règles non conformes

Affiche un graphique à barres horizontales comparant jusqu'à 10 packs de conformité au niveau du compte provenant de l'agrégateur sélectionné, par ordre décroissant du nombre de règles non conformes. Passez la souris sur le graphique pour voir le pourcentage de règles conformes et non conformes pour chaque pack de conformité au niveau du compte.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Les 10 meilleurs packs de conformité au niveau de l'organisation en termes de règles non conformes

Affiche un graphique à barres horizontales comparant jusqu'à 10 packs de conformité au niveau organisationnel provenant de l'agrégateur sélectionné, par ordre décroissant du nombre de règles non conformes. Passez la souris sur le graphique pour voir le pourcentage de règles conformes et non conformes dans chaque pack de conformité au niveau de l'organisation.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Les 10 meilleurs comptes en termes de règles non conformes dans l'ensemble des packs de conformité

Les 10 principaux comptes selon les règles non conformes dans les packs de conformité affichent un graphique à barres horizontales comparant jusqu'à 10 comptes de l'agrégateur sélectionné par ordre décroissant selon le nombre de règles non conformes dans l'ensemble de vos packs de

conformité. Passez la souris sur le graphique pour voir le nombre exact de règles non conformes dans chaque compte.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Tableau de bord d'inventaire

Consultez des tableaux de bord d’inventaire automatisés à l'aide des widgets qui résument les informations relatives aux données de configuration des ressources au sein de votre agrégateur.

Les 10 principaux types de ressources en fonction du nombre de ressources

Affiche un graphique à barres horizontales comparant jusqu'à 10 types de ressources de l'agrégateur sélectionné par ordre décroissant, en fonction du nombre de ressources. Passez le curseur sur le graphique pour consulter le nombre exact de ressources pour chaque type de ressource.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Nombre de ressources par région

Affiche un graphique à barres horizontales comparant jusqu'à 10 types de régions pour lesquelles l'agrégateur sélectionné collecte les données par ordre décroissant, en fonction du nombre de ressources. Passez le curseur sur le graphique pour consulter le nombre exact de ressources pour chaque région.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné.

10 principaux comptes en fonction du nombre de ressources

Affiche un graphique à barres horizontales comparant jusqu'à 10 comptes de l'agrégateur sélectionné par ordre décroissant, en fonction du nombre de ressources. Passez le curseur sur le graphique pour consulter le nombre exact de ressources pour chaque type de ressource.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données.

Nombre de ressources en fonction du type de ressource du service Amazon EC2

Affiche un graphique à barres horizontales comparant les types de ressources Amazon EC2 de l'agrégateur sélectionné par ordre décroissant, en fonction du nombre de ressources. Passez le curseur sur le graphique pour consulter le nombre exact de ressources pour chaque type de ressource Amazon EC2.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données. Pour utiliser ce graphique, vous devez configurer l'enregistreur pour enregistrer les types de ressources Amazon EC2. Pour plus d'informations, voir Sélection des AWS Config enregistrements de ressources.

Les 10 principaux types d'instances EC2 utilisés

Affiche un graphique à barres horizontales comparant jusqu'à 10 types d’instances Amazon EC2 de l'agrégateur sélectionné par ordre décroissant, en fonction de l’utilisation. Passez le curseur sur le graphique pour consulter l'utilisation de chaque type d'instance EC2.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données. Pour utiliser ce graphique, vous devez configurer l'enregistreur pour enregistrer les types de ressources d’instance EC2. Pour plus d'informations, consultez la section AWS Ressources de recodage.

Nombre de volumes EBS en fonction du type et de la taille du volume

Affiche un graphique à barres verticales comparant les volumes EBS de l'agrégateur sélectionné en fonction du nombre de ressources. Passez le curseur sur le graphique pour consulter le nombre et la répartition de la taille pour chaque type de volume EBS.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données. Pour utiliser ce graphique, vous devez configurer l'enregistreur pour enregistrer les types de ressources de volume EC2. Pour plus d'informations, voir Sélection des AWS Config enregistrements de ressources.

Nombre d'instances EC2 en cours d'exécution par rapport au nombre d'instances arrêtées par type

Affiche un graphique à barres horizontales comparant les types d'instances EC2 de l'agrégateur sélectionné en cours d'exécution aux instances EC2 arrêtées par type d'instance. Passez le curseur sur le graphique pour consulter le nombre exact d'instances EC2 arrêtées et en cours d'exécution pour chaque type.

Les données affichées dépendent des paramètres de l'enregistreur de configuration pour chaque compte de l'agrégateur sélectionné et des régions dans lesquelles l'agrégateur sélectionné est configuré pour collecter des données. Pour utiliser ce graphique, vous devez configurer l'enregistreur pour enregistrer les types de ressources d'instance EC2. Pour plus d'informations, consultez la section AWS Ressources de recodage.

Configuration d'un agrégateur à l'aide de la console

Dans la page Aggregator (Agrégateur), vous pouvez effectuer les actions suivantes :

- Créer un agrégateur en spécifiant les ID de compte source ou l'organisation et les régions dont vous voulez regrouper les données.
- Modifier et supprimer un agrégateur.

Rubriques

- Créer un agrégateur
- Modification d'un agrégateur
- Suppression d'un agrégateur

Créer un agrégateur

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Accédez à la page Agrégateurs et choisissez Créer un agrégateur.
3. Autoriser la réplication des données, autorise AWS Config la réplication des données des comptes sources vers un compte agrégateur.

Choisissez Autoriser AWS Config pour répliquer les données du ou des comptes source vers un compte agrégateur. Vous devez sélectionner cette case à cocher pour continuer à ajouter un agrégateur.

4. Pour Aggregator name (Nom de l'agrégateur), saisissez le nom de votre agrégateur.

   Le nom de l'agrégateur doit être un nom unique comportant au maximum 64 caractères alphanumériques. Le nom peut contenir des tirets et des traits de soulignement.

5. Pour Select source accounts (Sélectionner les comptes source), choisissez Add individual account IDs (Ajouter des ID de compte individuel) ou Add my organization (Ajouter mon organisation) pour indiquer l'emplacement depuis lequel vous souhaitez regrouper les données.

   > **Note**
   >
   > Une autorisation est requise lorsque vous utilisez l'option Ajouter des ID de compte individuel pour sélectionner des comptes sources.

   - Si vous choisissez Add individual account IDs (Ajouter des ID de compte individuel), vous pouvez indiquer les ID de compte individuel d'un compte agrégateur.
     1. Choisissez Add source accounts (Ajouter les comptes source) pour ajouter les ID de compte.
     2. Choisissez Ajouter des Compte AWS identifiants pour ajouter manuellement des identifiants séparés par des Compte AWS virgules. Si vous souhaitez regrouper les données du compte actuel, saisissez l'ID de ce compte.

        OU

        Choisissez Charger un fichier pour charger un fichier (.txt ou .csv) dont les identifiants sont séparés par des Compte AWS virgules.
     3. Choisissez Add source accounts (Ajouter les comptes source) pour confirmer votre sélection.
   - Si vous choisissez Add my organization (Ajouter mon organisation), vous pouvez ajouter tous les comptes de votre organisation à un compte agrégateur.

> **Note**
>
> Vous devez être connecté au compte de gestion ou à un administrateur délégué enregistré et toutes les fonctionnalités doivent être activées dans votre organisation. Si l'appelant est un compte de gestion, AWS Config appelle `EnableAwsServiceAccess` l'API pour permettre l'intégration entre AWS Config et AWS Organizations. Si l'appelant est un administrateur délégué enregistré, AWS Config appelle `ListDelegatedAdministrators` l'API pour vérifier s'il est un administrateur délégué valide.
> Assurez-vous que le compte de gestion enregistre l'administrateur délégué pour le nom principal du AWS Config service (config.amazonaws.com) avant que l'administrateur délégué ne crée un agrégateur. Pour enregistrer un administrateur délégué, consultez Enregistrer un administrateur délégué.

Vous devez attribuer un rôle IAM pour permettre d' AWS Config appeler des API en lecture seule pour votre organisation.

1. Choisissez Sélectionner un rôle dans votre compte pour choisir un rôle &IAM existant.

   > **Note**
   >
   > Dans la console IAM, attachez la stratégie gérée `AWSConfigRoleForOrganizations` à votre rôle IAM. L'attachement de cette politique AWS Config permet d'appeler AWS Organizations `DescribeOrganizationListAWSServiceAccessForOrganization`, et des `ListAccounts` API. Par défaut, `config.amazonaws.com` est automatiquement spécifié en tant qu'entité de confiance.

2. Choisissez Créer un rôle et saisissez un nom de rôle IAM pour créer le rôle IAM.

6. Pour Regions (Régions), choisissez les régions pour lesquelles vous souhaitez regrouper les données.

   - Sélectionnez une ou plusieurs régions ou toutes les Régions AWS.
   - Sélectionnez Inclure le futur Régions AWS pour agréger les données de tous les futurs Régions AWS où l'agrégation de données multi-comptes et multirégions est activée.

7. Choisissez Enregistrer. AWS Config affiche l'agrégateur.

Modification d'un agrégateur

1. Pour apporter des modifications à un agrégateur, choisissez le nom de l'agrégateur.
2. Choisissez Actions, puis Modifier.
3. Utilisez les sections de la page Modifier un agrégateur pour modifier les comptes source, les rôles IAM ou les régions de l'agrégateur.

> **Note**
>
> Vous ne pouvez pas modifier le type de source du ou des comptes individuels de l'organisation et inversement.

4. Choisissez Enregistrer.

Suppression d'un agrégateur

1. Pour supprimer un agrégateur, choisissez le nom de l'agrégateur.
2. Choisissez Actions, puis Delete (Supprimer).

   Un message d'avertissement s'affiche. La suppression d'un agrégateur entraîne la perte de toutes les données agrégées. Vous ne pouvez pas récupérer ces données, mais les données du ou des comptes source ne sont pas affectées.
3. Choisissez Supprimer pour confirmer votre sélection.

Configuration d'un agrégateur à l'aide du AWS Command Line Interface

Vous pouvez créer, afficher, mettre à jour et supprimer des données d' AWS Config agrégateur à l'aide de AWS Command Line Interface (AWS CLI).

AWS CLI Il s'agit d'un outil unifié pour gérer vos AWS services. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs AWS services depuis la ligne de commande et utiliser des scripts pour les automatiser. Pour plus d'informations sur les AWS CLI outils AWS CLI et pour obtenir des instructions sur leur installation, reportez-vous à ce qui suit dans le guide de AWS Command Line Interface l'utilisateur.

- AWS Command Line Interface Guide de l'utilisateur
- Préparation de l'installation de l' AWS Command Line Interface

Si nécessaire, entrez `aws configure` pour configurer le AWS CLI afin d'utiliser une AWS région dans laquelle des agrégateurs sont disponibles.

Rubriques

- Ajout d'un agrégateur à l'aide de comptes individuels
- Ajout d'un agrégateur à l'aide d' AWS Organizations
- Enregistrer un administrateur délégué
- Affichage d'un agrégateur
- Modification d'un agrégateur
- Suppression d'un agrégateur

Ajout d'un agrégateur à l'aide de comptes individuels

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Saisissez la commande suivante pour créer un agrégateur nommé **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

   Pour `account-aggregation-sources`, indiquez l'un des éléments suivants.

   - Liste d' Compte AWS identifiants séparés par des virgules pour lesquels vous souhaitez agréger les données. Placez les ID de compte entre crochets avec une mise en échappement (par exemple, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\", \"AccountID3\"],\"AllAwsRegions\": true}]"`).
   - Vous pouvez également télécharger un fichier JSON contenant des identifiants séparés par des Compte AWS virgules. Pour charger le fichier, utilisez la syntaxe suivante : `--account-aggregation-sources MyFilePath/MyFile.json`

     Le format du fichier JSON doit être le suivant :

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Appuyez sur Entrée pour exécuter la commande.

   Vous devez voir des résultats similaires à ce qui suit :

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Ajout d'un agrégateur à l'aide d' AWS Organizations

Avant de commencer cette procédure, vous devez être connecté au compte de gestion ou à un administrateur délégué enregistré et toutes les fonctionnalités doivent être activées dans votre organisation.

> **Note**
>
> Assurez-vous que le compte de gestion enregistre un administrateur délégué portant les deux noms principaux de AWS Config service suivants (`config.amazonaws.cometconfig-multiaccountsetup.amazonaws.com`) avant que l'administrateur délégué ne crée un agrégateur. Pour enregistrer un administrateur délégué, consultez Enregistrer un administrateur délégué.

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Si vous n'avez pas créé de rôle IAM pour votre AWS Config agrégateur, entrez la commande suivante :

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> Copiez le nom de ressource Amazon (ARN) à partir de ce rôle IAM pour l'utiliser lors de la création de votre AWS Config agrégateur. Vous pouvez trouver l'ARN sur l'objet de réponse.

3. Si aucune stratégie n'est associée à votre rôle IAM, associez la stratégie AWSConfigRoleForOrganizationsgérée ou entrez la commande suivante :

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAWSSe
```

4. Saisissez la commande suivante pour créer un agrégateur nommé **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Appuyez sur Entrée pour exécuter la commande.

Vous devez voir des résultats similaires à ce qui suit :

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Enregistrer un administrateur délégué

Les administrateurs délégués sont des comptes au sein d'une AWS organisation donnée auxquels des privilèges administratifs supplémentaires sont accordés pour un AWS service spécifique.

1. Connectez-vous avec les informations d'identification du compte de gestion.
2. Ouvrez une invite de commande ou une fenêtre de terminal.
3. Entrez la commande suivante pour activer l'accès au service en tant qu'administrateur délégué afin de déployer et de gérer les AWS Config règles et les packs de conformité au sein de votre organisation :

   ```
   aws organizations enable-aws-service-access --service-principal=config-
   multiaccountsetup.amazonaws.com
   ```

4. Entrez la commande suivante pour activer l'accès au service en tant qu'administrateur délégué de votre organisation afin d'agréger AWS Config les données au sein de votre organisation :

   ```
   aws organizations enable-aws-service-access --service-
   principal=config.amazonaws.com
   ```

5. Pour vérifier si l’accès au service est bien activé, saisissez la commande suivante et appuyez sur Entrée pour l’exécuter.

```
aws organizations list-aws-service-access-for-organization
```

Vous devez voir des résultats similaires à ce qui suit :

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. Saisissez ensuite la commande suivante pour enregistrer un compte membre en tant qu'administrateur délégué pour AWS Config.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

and

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. Pour vérifier si l'administrateur délégué est bien enregistré, saisissez la commande suivante à partir du compte de gestion et appuyez sur Entrée pour l'exécuter.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

and

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

Vous devez voir des résultats similaires à ce qui suit :

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::MemberAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

Affichage d'un agrégateur

1. Entrez la commande suivante :

```
aws configservice describe-configuration-aggregators
```

2. En fonction de votre compte source, vous devez voir une sortie similaire à ce qui suit :

   Pour les comptes individuels

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
```

```
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

OU

Pour une organisation

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Modification d'un agrégateur

1. Vous pouvez utiliser la commande `put-configuration-aggregator` pour mettre à jour ou modifier un agrégateur de configuration.

   Saisissez la commande suivante pour ajouter un nouvel ID de compte à **`MyAggregator`** :

   ```
   aws configservice put-configuration-aggregator --configuration-aggregator-name
    MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
   \"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
   ```

2. En fonction de votre compte source, vous devez voir une sortie similaire à ce qui suit :

   Pour les comptes individuels

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

OU

Pour une organisation

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Suppression d'un agrégateur

Entrez la commande suivante :

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

En cas de réussite, la commande s'exécute sans sortie supplémentaire.

Autoriser les comptes agrégateurs à collecter des données de AWS Config configuration et de conformité à l'aide de la console

AWS Config vous permet d'autoriser les comptes à collecter des données AWS Config de configuration et de conformité.

Sur la page Authorisations, vous pouvez effectuer les actions suivantes :

- Ajouter une autorisation pour autoriser un compte et une région Aggregator à collecter des données AWS Config de configuration et de conformité de votre compte actuel.
- Autoriser une demande en attente d'un compte Aggregator pour collecter des données AWS Config de configuration et de conformité de votre compte actuel.
- Supprimer une autorisation accordée à un compte Aggregator lui permettant de collecter des données AWS Config de configuration et de conformité de votre compte actuel.

Rubriques

- Considérations
- Ajout d'une autorisation pour des comptes et des régions Aggregator
- Autorisation d'une demande en attente pour un compte Aggregator
- Suppression d'une autorisation pour un compte Aggregator existant

Considérations

Il existe deux types d'agrégateurs : l'agrégateur de comptes individuels et l'agrégateur Organization

Un agrégateur de comptes individuel nécessite une autorisation pour tous les comptes et régions sources que vous souhaitez inclure, y compris les comptes et les régions externes, ainsi que les régions et les comptes membres de l'organisation.

Pour un agrégateur d'organisations, aucune autorisation n'est requise pour les régions des comptes membres de l'organisation, car l'autorisation est intégrée au AWS Organizations service.

Les agrégateurs ne s'activent pas automatiquement AWS Config en votre nom

AWS Config doit être activé dans le compte source et dans la région pour l'un ou l'autre type d'agrégateur, afin que les AWS Config données soient générées dans le compte source et dans la région.

Ajout d'une autorisation pour des comptes et des régions Aggregator

Vous pouvez ajouter une autorisation pour autoriser les comptes agrégateurs et les régions à collecter des données de AWS Config configuration et de conformité.

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Accédez à la page Autorisations et choisissez Ajouter une autorisation.
3. En regard de Compte Aggregator, entrez l'ID de compte à 12 chiffres d'un compte Aggregator.
4. Pour la région de l'agrégateur, choisissez l' Régions AWS endroit où le compte de l'agrégateur est autorisé à collecter les données de AWS configuration et de conformité.
5. Choisissez Ajouter une autorisation pour confirmer votre sélection.

   AWS Config affiche un compte agrégateur, une région et un statut d'autorisation.

> **Note**
>
> Vous pouvez également ajouter des autorisations aux comptes agrégateurs et aux régions par programmation à l'aide AWS CloudFormation d'exemples de modèles. Pour plus d'informations, consultez AWS::Config::AggregationAuthorizationle guide de AWS CloudFormation l'utilisateur.

Autorisation d'une demande en attente pour un compte Aggregator

Si vous avez une demande d'autorisation en attente d'un compte Aggregator existant, vous verrez l'état de la demande sur la page Autorisations. Vous pouvez autoriser une demande en attente à partir de cette page.

1. Choisissez le compte Aggregator que vous souhaitez autoriser, puis choisissez Autoriser.

   Un message de confirmation s'affiche pour confirmer que vous souhaitez autoriser le compte agrégateur à collecter des AWS Config données à partir de ce compte.
2. Choisissez à nouveau Autoriser pour confirmer que vous souhaitez accorder l'autorisation au compte Aggregator.

   L'état de l'autorisation passe de Demande d'autorisation à Autorisé.

Période d'approbation de l'autorisation

L'approbation d'une autorisation est requise pour ajouter des comptes sources à un agrégateur de comptes individuel. Une demande d'approbation d'autorisation en attente sera disponible pendant 7 jours après l’ajout d’un compte source par un agrégateur de comptes individuel.

Suppression d'une autorisation pour un compte Aggregator existant

1. Choisissez le compte Aggregator dont vous souhaitez supprimer l’autorisation, puis choisissez Supprimer.

   Un message d'avertissement s'affiche. Lorsque vous supprimez cette autorisation, AWS Config les données ne seront plus partagées avec le compte agrégateur.
2. Choisissez Supprimer pour confirmer votre sélection.

   Le compte Aggregator est supprimé.

Une fois que l'autorisation d'un compte Aggregator est supprimée, les données restent dans le compte Aggregator pendant 24 heures avant d'être supprimées.

Autoriser les comptes agrégateurs à collecter des données de AWS Config configuration et de conformité à l'aide du AWS Command Line Interface

Vous pouvez autoriser les comptes agrégateurs à collecter des AWS Config données à partir des comptes sources et à supprimer des comptes agrégateurs à l'aide du AWS Command Line Interface ()AWS CLI. Pour utiliser la console AWS de gestion, voirAutoriser les comptes agrégateurs à collecter des données de AWS Config configuration et de conformité à l'aide de la console.

AWS CLI Il s'agit d'un outil unifié pour gérer vos AWS services. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs AWS services depuis la ligne de commande et utiliser des scripts pour les automatiser. Pour plus d'informations sur les AWS CLI outils AWS CLI et pour obtenir des instructions sur leur installation, reportez-vous à ce qui suit dans le guide de AWS Command Line Interface l'utilisateur.

- AWS Command Line Interface Guide de l'utilisateur
- Préparation de l’installation de l’ AWS Command Line Interface

Si nécessaire, saisissez `aws configure` pour configurer le AWS CLI afin d'utiliser une AWS région dans laquelle des packs de AWS Config conformité sont disponibles.

Rubriques

- Considérations
- Ajout d'une autorisation pour des comptes et des régions Aggregator
- Suppression d'un compte d'autorisation

Considérations

Il existe deux types d'agrégateurs : l'agrégateur de comptes individuels et l'agrégateur Organization

Un agrégateur de comptes individuel nécessite une autorisation pour tous les comptes et régions sources que vous souhaitez inclure, y compris les comptes et les régions externes, ainsi que les régions et les comptes membres de l'organisation.

Pour un agrégateur d'organisations, aucune autorisation n'est requise pour les régions des comptes membres de l'organisation, car l'autorisation est intégrée au AWS Organizations service.

Les agrégateurs ne s'activent pas automatiquement AWS Config en votre nom

AWS Config doit être activé dans le compte source et dans la région pour l'un ou l'autre type d'agrégateur, afin que les AWS Config données soient générées dans le compte source et dans la région.

Ajout d'une autorisation pour des comptes et des régions Aggregator

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez la commande suivante :

```
aws configservice put-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

3. Vous devez voir des résultats similaires à ce qui suit :

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

Suppression d'un compte d'autorisation

Entrez la commande suivante :

```
aws configservice delete-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

En cas de réussite, la commande s'exécute sans sortie supplémentaire.

Interrogation de l'état de configuration actuel des ressources AWS

Présentation d'une fonctionnalité d'aperçu pour les requêtes avancées qui vous permet d'utiliser les fonctionnalités de l'intelligence artificielle générative (IA générative) pour saisir des instructions dans un anglais simple et les convertir dans un format de ready-to-use requête. Pour plus d'informations, consultez Processeur de requêtes en langage naturel pour les requêtes avancées.

Vous pouvez l'utiliser AWS Config pour interroger l'état de configuration actuel des AWS ressources en fonction des propriétés de configuration d'un seul compte et d'une seule région ou de plusieurs comptes et régions. Vous pouvez effectuer des requêtes basées sur les propriétés par rapport aux métadonnées de l'état actuel des AWS ressources dans une liste de ressources prises en charge. AWS Config Pour plus d'informations sur la liste des types de ressources pris en charge, consultez Types de ressources pris en charge pour les requêtes avancées.

Les requêtes avancées fournissent un point de terminaison de requête unique et un langage de requête pour obtenir les métadonnées de l'état actuel des ressources sans effectuer d'appels d'API de description spécifiques au service. Vous pouvez utiliser des agrégateurs de configuration pour exécuter les mêmes requêtes à partir d'un compte central sur plusieurs comptes et AWS régions.

Rubriques

- Fonctionnalités
- Composants d'une requête
- Exemples de requêtes
- Exemples de requêtes relationnelles
- Limites
- Prise en charge de la région
- Interrogation à l'aide de l'éditeur de requête SQL (console)
- Requête à l'aide de l'éditeur de requête SQL (AWS CLI)
- Processeur de requêtes en langage naturel pour les requêtes avancées

Fonctionnalités

AWS Config utilise un sous-ensemble de la `SELECT` syntaxe du langage de requête structuré (SQL) pour effectuer des requêtes basées sur les propriétés et des agrégations sur les données des éléments de configuration (CI) actuels. La complexité des requêtes varie, allant de correspondances avec des identifiants de balises et/ou de ressources à des requêtes plus complexes, telles que l'affichage de tous les compartiments Amazon S3 dont le versionnement est désactivé. Cela vous permet d'obtenir exactement l'état actuel de la ressource dont vous avez besoin sans effectuer d'appels d'API spécifiques au service AWS .

Il prend en charge les fonctions d'agrégation telles que `AVG`, `COUNT`, `MAX`, `MIN` et `SUM`.

Vous pouvez utiliser une requête avancée pour :

- la gestion des stocks : par exemple, pour récupérer la liste des instances Amazon EC2 d'une taille particulière.
- la sécurité et l'intelligence opérationnelle : par exemple, pour récupérer la liste des ressources dont une propriété de configuration spécifique est activée ou désactivée.
- l'optimisation des coûts : par exemple, pour dresser la liste des volumes Amazon EBS qui ne sont attachés à aucune instance EC2.
- Données de conformité ; par exemple, pour récupérer une liste de tous vos packs de conformité et de leur statut de conformité.

Pour plus d'informations sur l'utilisation du langage de requête AWS SQL, voir Qu'est-ce que le langage SQL (langage de requête structuré) ? .

Composants d'une requête

Les composants de la requête SQL `SELECT` sont les suivants.

Résumé

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

Paramètres

[Condition WHERE]

Filtre les résultats en fonction de la `condition` que vous spécifiez.

[GROUP BY property]

Agrège le jeu de résultats en groupes de lignes avec des valeurs correspondantes pour la propriété donnée.

La clause GROUP BY s'applique aux agrégations.

[ORDER BY property [ASC | DESC] [, property [ASC | DESC] ...]]

Trie un jeu de résultats par une ou `properties` de sortie.

Lorsque la clause contient plusieurs propriétés, le jeu de résultats est trié selon le premier élément `property`, puis selon le deuxième élément `property` pour les lignes ayant des valeurs correspondantes pour la première propriété, et ainsi de suite.

Exemples

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

Exemples de requêtes

Query to list all EC2 instances with AMI ID ami-12345

Interrogation :

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
```

```
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Résultats :

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
```

```
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

Interrogation :

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

Résultats :

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

Interrogation :

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Résultats :

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

Interrogation :

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Résultats :

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

Interrogation :

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
```

```
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

Résultats :

```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
```

```
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Exemples de requêtes relationnelles

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

OU

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

Limites

> **Note**
>
> La requête avancée ne prend pas en charge l'interrogation de ressources qui n'ont pas été configurées pour être enregistrées par l'enregistreur de configuration. AWS Config crée des éléments de configuration (CI) `ResourceNotRecorded` dans le `configurationItemStatus` lorsqu'une ressource a été découverte mais n'est pas configurée pour être enregistrée par l'enregistreur de configuration. Bien qu'un agrégateur agrège ces CI, les requêtes avancées ne permettent pas d'interroger les CI avec `ResourceNotRecorded`. Mettez à jour les paramètres de votre enregistreur afin d'activer l'enregistrement des types de ressources que vous souhaitez interroger.

En tant que sous-ensemble de la commande SQL `SELECT`, la syntaxe de requête présente les limitations suivantes :

- Pas de prise en charge pour les mots clés `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN` et `UNION` mots clés dans une requête. Les requêtes de valeur `NULL` ne sont pas prises en charge.
- Pas de prise en charge des requêtes sur des ressources tierces. Les ressources tierces récupérées à l'aide de requêtes avancées auront le champ de configuration défini comme `NULL`.
- Pas de prise en charge des structures imbriquées (comme les balises) à décompresser avec des requêtes SQL.
- La notation CIDR est convertie en plages d'adresses IP pour la recherche. Cela signifie que `"="` et `"BETWEEN"` recherchent toute plage qui inclut l'adresse IP fournie, plutôt qu'une adresse exacte. Pour rechercher une plage exacte d'adresses IP, vous devez ajouter des conditions supplémentaires afin d'exclure les adresses IP situées en dehors de cette plage. Par exemple,

pour rechercher 10.0.0.0/24 et uniquement ce bloc d'adresses IP, vous pouvez procéder comme suit :

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Pour 192.168.0.2/32, vous pouvez effectuer une recherche similaire :

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

- Lors de l'interrogation de plusieurs propriétés dans un tableau d'objets, les correspondances sont calculées sur les éléments de tableau. Par exemple, pour une ressource R avec des règles A et B, la ressource est conforme à la règle A, mais non conforme à la règle B. La ressource R est stockée sous la forme suivante :

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R sera renvoyée par cette requête :

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

La première condition `configuration.configRuleList.complianceType = 'non_compliant'` est appliquée à TOUS les éléments de R.configRuleList, car R possède une règle (règle B) avec ComplianceType = 'non_compliant', la condition est évaluée comme vraie. La deuxième condition `configuration.configRuleList.configRuleName` est appliquée à TOUS les éléments de R.configRuleList, car R a une règle (règle A) avec configRuleName = « A », la condition est évaluée comme vraie. Comme les deux conditions sont vraies, R sera renvoyée.

- La commande `SELECT` raccourcie permettant de sélectionner toutes les colonnes (à savoir `SELECT *`) sélectionne uniquement les propriétés scalaires de niveau supérieur d'un élément de configuration. Les propriétés scalaires renvoyées sont `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType` et `version`.
- Limitations propres aux caractères génériques :
  - Les caractères génériques sont pris en charge uniquement pour les valeurs de propriété et non pour les clés de propriété (par exemple, `...WHERE someKey LIKE 'someValue%'` est pris en charge, mais `...WHERE 'someKey%' LIKE 'someValue%'` n'est pas pris en charge).
  - Prise en charge uniquement des caractères génériques en suffixe (par exemple, `...LIKE 'AWS::EC2::%'` et `...LIKE 'AWS::EC2::_'` sont pris en charge, mais `...LIKE '%::EC2::Instance'` et `...LIKE '_::EC2::Instance'` ne sont pas pris en charge).
  - Les correspondances d'un caractère générique doivent compter au moins trois caractères (par exemple, `...LIKE 'ab%'` et `...LIKE 'ab_'` ne sont pas autorisés, alors que `...LIKE 'abc%'` et `...LIKE 'abc_'` le sont).

> **Note**
>
> Le « _ » (tiret du bas simple) est également traité comme un caractère générique.

- Limitations propres aux agrégations :
  - Les fonctions d'agrégation peuvent accepter un seul argument ou une seule propriété.
  - Les fonctions d'agrégation ne peuvent pas accepter d'autres fonctions comme arguments.
  - `GROUP BY` avec une clause `ORDER BY` faisant référence à des fonctions d'agrégation ne peut contenir qu'une seule propriété.
  - Pour toutes les autres agrégations, les clauses `GROUP BY` peuvent contenir jusqu'à trois propriétés.

- La pagination est prise en charge pour toutes les requêtes agrégées, sauf lorsque la clause `ORDER BY` comporte une fonction d'agrégation. Par exemple, `GROUP BY X, ORDER BY Y` ne fonctionne pas si `Y` est une fonction d'agrégation.
- Pas de prise en charge des clauses `HAVING` dans les agrégations.

- Limites des identifiants non concordants :

  Les identifiants non concordants sont des propriétés qui ont la même orthographe mais une casse différente (majuscules et minuscules). La requête avancée ne permet pas de traiter les requêtes qui contiennent des identifiants non concordants. Par exemple :

  - Deux propriétés qui ont exactement la même orthographe, mais une casse différente (`configuration.dbclusterIdentifier` et `configuration.dBClusterIdentifier`).
  - Deux propriétés où l'une est un sous-ensemble de l'autre et qui ont une casse différente (`configuration.ipAddress` et `configuration.ipaddressPermissions`).

Prise en charge de la région

Les requêtes avancées sont prises en charge dans les régions suivantes :

Nom de la région	Région	Point de terminaison	Protocole
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Afrique (Le Cap)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asie-Pacifique (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Asie-Pacifique (Jakarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Asie-Pacifique (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Asie-Pacifique (Singapour)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Canada Ouest (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europe (Milan)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole
Europe (Espagne)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europe (Zurich)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israël (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Moyen-Orient (Bahreïn)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Moyen-Orient (EAU)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (USA Est)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (US-Ouest)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Interrogation à l'aide de l'éditeur de requête SQL (console)

Présentation d'une fonctionnalité d'aperçu pour les requêtes avancées qui vous permet d'utiliser les fonctionnalités de l'intelligence artificielle générative (IA générative) pour saisir des instructions dans un anglais simple et les convertir dans un format de ready-to-use requête. Pour plus d'informations, consultez Processeur de requêtes en langage naturel pour les requêtes avancées.

Vous pouvez soit utiliser des AWS exemples de requêtes, soit créer votre propre requête appelée requêtes personnalisées.

Considérations

Prérequis

Si vous utilisez l'une des politiques AWS gérées suivantes, vous aurez les autorisations nécessaires pour exécuter et enregistrer une requête : AWSServiceRoleForConfig(rôle lié au service) ou AWS_ConfigRole

Dans le cas contraire, vous devez disposer des autorisations incluses dans la politique AWSConfigUserAccess AWS gérée.

Liste des propriétés que vous pouvez interroger

Une liste actualisée des propriétés et de leurs types de données est disponible dans GitHub.

Requêtes avancées et agrégateurs

Pour exécuter une requête sur un agrégateur, créez un agrégateur. Pour plus d'informations, consultez Configuration d'un agrégateur à l'aide de la console.

Si un agrégateur est déjà configuré, dans l'étendue de la requête, choisissez l'agrégateur pour exécuter une requête avancée sur cet agrégateur. Lorsque vous sélectionnez un agrégateur, pensez à ajouter l' Compte AWS ID et la AWS région dans l'instruction de requête pour afficher ces informations dans les résultats.

Utiliser un AWS exemple de requête

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.

2. Choisissez Requêtes avancées dans la navigation de gauche pour interroger vos configurations de ressources pour un seul compte et une seule région ou pour plusieurs comptes et régions.
3. Sur la page Requêtes avancées, choisissez une requête appropriée dans la liste des requêtes. Vous pouvez filtrer les requêtes de la liste en fonction de leur nom, de leur description, de leur créateur ou de leurs balises. Pour filtrer les requêtes AWS , choisissez Créateur et saisissez AWS. La requête sélectionnée s'affiche dans l'éditeur de requête SQL. Vous pouvez la modifier en fonction de vos besoins.
4. Pour enregistrer cette requête dans une nouvelle requête, choisissez Enregistrer sous.
   - Dans le champ Nom de la requête, mettez à jour le nom de la requête.
   - Dans le champ Description, mettez à jour la description.
   - Saisissez jusqu'à 50 balises uniques pour cette requête.
   - Choisissez Enregistrer.
5. Cliquez sur Exécuter. Les résultats de la requête sont affichés dans le tableau figurant sous l'éditeur de requête.
6. Choisissez Exporter comme pour exporter les résultats de la requête au format CSV ou JSON.

> **Note**
>
> Les résultats de la requête sont paginés. L'export permet d'exporter jusqu'à 500 résultats.
> Vous pouvez également utiliser les API pour récupérer tous les résultats. Les résultats sont paginés et vous pouvez récupérer 100 résultats à la fois.

Création de votre requête personnalisée

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Requêtes avancées dans la navigation de gauche pour interroger vos configurations de ressources pour un seul compte et une seule région ou pour plusieurs comptes et régions.
3. Pour créer votre requête personnalisée, choisissez Nouvelle requête.

   Pour afficher ou modifier une requête personnalisée, filtrez une requête en fonction de son nom, de sa description, de son créateur ou de ses balises. Pour filtrer les requêtes personnalisées, choisissez Créateur et saisissez Personnalisé.

4. Sur la page Éditeur de requête, créez votre propre requête pour ce compte et cette Région. Vous pouvez également sélectionner un agrégateur approprié pour créer une requête pour plusieurs comptes et régions.
5. Vous pouvez apporter des modifications à cette requête. Choisissez Enregistrer pour enregistrer cette requête.
   - Dans le champ Nom de la requête, mettez à jour le nom de la requête.
   - Dans le champ Description, mettez à jour la description.
   - Saisissez jusqu'à 50 balises uniques pour cette requête.
   - Choisissez Enregistrer.
6. Cliquez sur Exécuter. Les résultats de la requête sont affichés dans le tableau figurant sous l'éditeur de requête.
7. Choisissez Exporter comme pour exporter les résultats de la requête au format CSV ou JSON.

   Les résultats de la requête sont paginés. L’export permet d’exporter jusqu’à 500 résultats.

   Vous pouvez également utiliser les API pour récupérer tous les résultats. Les résultats sont paginés et vous pouvez récupérer 100 résultats à la fois.

Requête à l'aide de l'éditeur de requête SQL (AWS CLI)

AWS CLI Il s'agit d'un outil unifié pour gérer vos AWS services. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs AWS services depuis la ligne de commande et utiliser des scripts pour les automatiser. Pour plus d'informations sur les AWS CLI outils AWS CLI et pour obtenir des instructions sur leur installation, reportez-vous à ce qui suit dans le guide de AWS Command Line Interface l'utilisateur.

- AWS Command Line Interface Guide de l'utilisateur
- Préparation de l’installation de l’ AWS Command Line Interface

Si nécessaire, entrez `aws configure` pour configurer le AWS CLI afin d'utiliser une AWS région dans laquelle des requêtes avancées sont disponibles.

Considérations

Prérequis

Si vous utilisez l'une des politiques AWS gérées suivantes, vous aurez les autorisations nécessaires pour exécuter et enregistrer une requête : AWSServiceRoleForConfig(rôle lié au service) ou AWS_. ConfigRole

Dans le cas contraire, vous devez disposer des autorisations incluses dans la politique AWSConfigUserAccess AWS gérée.

Liste des propriétés que vous pouvez interroger

Une liste actualisée des propriétés et de leurs types de données est disponible dans GitHub.

Requêtes avancées et agrégateurs

Pour exécuter une requête sur un agrégateur, créez un agrégateur. Pour plus d'informations, consultez Configuration d'un agrégateur à l'aide de la console.

Si un agrégateur est déjà configuré, dans l'étendue de la requête, choisissez l'agrégateur pour exécuter une requête avancée sur cet agrégateur. Lorsque vous sélectionnez un agrégateur, pensez à ajouter l' Compte AWS ID et la AWS région dans l'instruction de requête pour afficher ces informations dans les résultats.

Interrogation des données de configuration des ressources

Pour interroger vos données de configuration de ressources à l'aide de l'éditeur de requête (AWS CLI) pour un seul compte et une seule région

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez la commande suivante pour interroger les données de configuration de vos ressources.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

Selon la requête, la sortie peut ressembler à ce qui suit.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
```

```
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

Pour interroger vos données de configuration de ressources à l'aide de l'éditeur de requête (AWS CLI) pour plusieurs comptes et régions

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez la commande suivante pour interroger les données de configuration de vos ressources.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

Selon la requête, la sortie peut ressembler à ce qui suit.

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
```

```
}
```

> **Note**
>
> Lorsque vous utilisez les types de `AWS::IAM::Policy` ressources `AWS::IAM::User` `AWS::IAM::GroupAWS::IAM::Role`,, et dans une requête avancée, utilisez`awsRegion = 'global'`.

Enregistrement d'une requête

1. Ouvrez une invite de commande ou une fenêtre de terminal.
2. Entrez la commande suivante pour enregistrer une requête.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. Selon la requête, la sortie peut ressembler à ce qui suit.

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> Le paramètre `--tags` est facultatif. Lorsque vous transmettez les balises, les balises enregistrées ne seront pas renvoyées par `list-stored-queries` ou `get-stored-query`. Vous devez utiliser `list-tag-for-resources` pour récupérer les balises associées à une requête enregistrée.
> `--description` est un champ facultatif lors de la création ou de la mise à jour d'une requête.

Affichage de toutes les requêtes enregistrées

1. Entrez la commande suivante pour afficher la liste de toutes les requêtes enregistrées.

```
aws configservice list-stored-queries
```

2. Selon la requête, la sortie peut ressembler à ce qui suit.

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

Obtention des détails d'une requête enregistrée

1. Entrez la commande suivante pour obtenir les détails d'une requête enregistrée spécifique.

```
aws configservice get-stored-query --query-name cli-test
```

2. Selon la requête, la sortie peut ressembler à ce qui suit.

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
```

```
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

Suppression d'une requête enregistrée

- Entrez la commande suivante pour supprimer votre requête enregistrée.

```
aws configservice delete-stored-query --query-name cli-test
```

En cas de réussite, la commande s'exécute sans sortie supplémentaire.

Processeur de requêtes en langage naturel pour les requêtes avancées

> Le processeur de requêtes en langage naturel pour les requêtes avancées est en version préliminaire AWS Config et est sujet à modification.

Le processeur de requêtes en langage naturel pour les requêtes avancées utilise Amazon Bedrock, une technologie d'intelligence artificielle générative (IA générative) qui vous permet de saisir des instructions dans un anglais simple et de les convertir dans un format de ready-to-use requête. Avec le processeur de requêtes en langage naturel, vous pouvez interroger votre organisation Compte AWS ou l'ensemble d'une AWS organisation.

Une invite peut être une question ou une déclaration. Par exemple, vous pouvez saisir des instructions telles que « Quels équilibreurs de charge sont créés après le 1er janvier 2024 ? » et « Liste toutes mes fonctions lambda qui exécutent le nœud js 16. »

Considérations

Le processeur de requêtes en langage naturel ne peut pas effectuer les actions suivantes :

- Générez des requêtes à partir de langues autres que l'anglais.
- Générez des requêtes à partir d'invites qui ne concernent pas les requêtes avancées.

- Générez des requêtes à partir d'invites de plus de 1 000 caractères.
- Générez des requêtes à partir de corrections de suivi ou de sessions précédentes.
- Expliquez le code qui a été généré.

Requête à l'aide du processeur de requêtes en langage naturel

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Requêtes avancées dans la navigation de gauche pour interroger vos configurations de ressources pour un seul compte et une seule région ou pour plusieurs comptes et régions.
3. Sur la page Requêtes avancées, choisissez Nouvelle requête pour accéder à l'éditeur de requête .
   - (Facultatif) Pour exécuter une requête sur un agrégateur, créez un agrégateur. Pour plus d'informations, consultez Configuration d'un agrégateur à l'aide de la console.
   - Si vous avez déjà configuré un agrégateur, choisissez-le dans le périmètre de la requête afin d'exécuter une requête avancée sur lui. Lorsque vous sélectionnez un agrégateur, pensez à ajouter l' Compte AWS ID et la AWS région dans l'instruction de requête pour afficher ces informations dans les résultats.
4. Dans l'éditeur de requête, accédez à la section Processeur de requêtes en langage naturel. Entrez une invite en anglais simple, puis choisissez Generate. Pour des exemples, voir Exemples d'invites.
5. Après avoir généré une requête, vous pouvez choisir Copier (fonctionnellement équivalent à Ctrl +C) pour copier la requête dans votre presse-papiers, ou Remplir dans l'éditeur. Si la requête générée est renseignée dans l'éditeur, vous pouvez la modifier en fonction de vos besoins.
6. Pour enregistrer cette requête dans une nouvelle requête, choisissez Enregistrer sous.
   - Dans le champ Nom de la requête, mettez à jour le nom de la requête.
   - Dans le champ Description, mettez à jour la description.
   - Saisissez jusqu'à 50 balises uniques pour cette requête.
   - Choisissez Enregistrer.
7. Cliquez sur Exécuter. Les résultats de la requête s'affichent dans le tableau figurant sous l'éditeur de requête.
8. Choisissez Exporter comme pour exporter les résultats de la requête au format CSV ou JSON.

> **Note**
>
> Les résultats de la requête sont paginés. L'export permet d'exporter jusqu'à 500 résultats.
> Vous pouvez également utiliser les API pour récupérer tous les résultats. Les résultats sont paginés et vous pouvez récupérer 100 résultats à la fois.

Exemples d'instructions

Vous trouverez ci-dessous des instructions et des requêtes de génération que vous pouvez utiliser comme exemples.

Example: Quels équilibreurs de charge ont été créés après le 1er janvier 2024 ?

Prompt : What load balancers were created after January 1, 2024?

Requête générée :

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: Parmi mes instances de base de données RDS, lesquelles sont accessibles au public ?

Prompt : Which of my RDS database instances are publicly accessible?

Requête générée :

```
SELECT
    resourceId,
```

```
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: Combien d'instances EC2 ont été créées au cours de l'année écoulée ?

Prompt : How many EC2 instances were created in last one year?

Requête générée :

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: Combien d'instances EC2 ai-je dans chacune de mes Comptes AWS instances ?

Prompt : How many EC2 instances do I have in each of my Comptes AWS?

Requête générée :

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: Quels rôles IAM sont associés à la politique gérée AdministratorAccess ?

Prompt : Which IAM roles have the managed policy AdministratorAccess attached?

Requête générée :

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: Volumes EBS sans chiffrement

Prompt : EBS volumes without encryption

Requête générée :

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: Obtenez des ressources non conformes

Prompt : Get noncompliant resources

Requête générée :

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: Liste toutes mes fonctions lambda qui exécutent node js 16

Prompt : List all my lambda function that is running node js 16

Requête générée :

```
SELECT
```

```
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: Quels certificats ACM expireront dans les 30 prochains jours ?

Prompt : What ACM certificates expire the next 30 days?

Requête générée :

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> Les heures indiquées dans la requête générée dépendent de l'heure à laquelle vous entrez l'invite.

Fournir des commentaires

Vous pouvez fournir des commentaires généraux sur le processeur de requêtes en langage naturel ou des commentaires sur une requête spécifique générée.

Fournir des commentaires sur le processeur de requêtes en langage naturel

Cliquez sur le bouton Fournir des commentaires qui apparaît au-dessus du processeur de requêtes en langage naturel à droite. Vous pouvez saisir votre satisfaction ou votre insatisfaction et fournir des commentaires sur la manière de AWS Config rendre la requête en langage naturel plus utile.

> **Note**
>
> Ne divulguez aucune information personnelle, commercialement sensible ou confidentielle.

Fournir des commentaires sur une requête spécifique générée

Vous pouvez donner votre avis sur une requête générée en cliquant sur le bouton pouce vers le haut ou pouce bas qui apparaît sous la requête générée.

Prise en charge de la région

Le processeur de requêtes en langage naturel est pris en charge dans les régions suivantes.

Nom de la région	Région	Point de terminaison	Protocole
US East (Virginie du Nord)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
USA Ouest (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Supprimer des AWS Config données

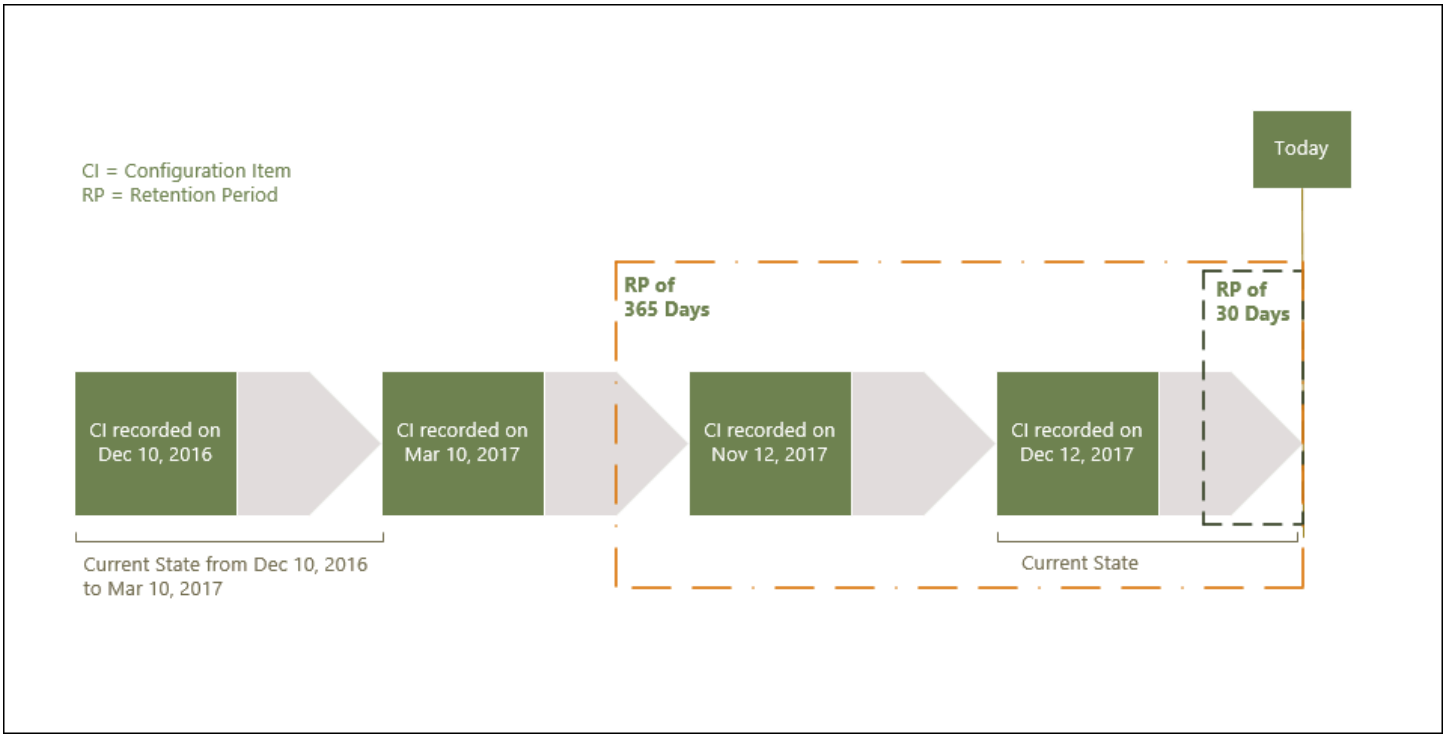
> **Note**
>
> While AWS Config utilise Amazon Simple Storage Service (Amazon S3) et Amazon Simple Notification Service (Amazon SNS) pour envoyer des instantanés de configuration et des AWS Config fichiers d'historique de configuration, mais dispose de ses propres politiques de stockage et de conservation des données. Les informations de cette page sont spécifiques à AWS Config. Amazon S3 et Amazon SNS appliquent leurs propres politiques distinctes en matière de stockage et de conservation de données.

AWS Config vous permet de supprimer vos données en spécifiant une période de conservation pour votre`ConfigurationItems`. Lorsque vous spécifiez une période de conservation, AWS Config elle conserve `ConfigurationItems` la vôtre pendant cette période spécifiée. Vous pouvez choisir une période comprise entre un minimum de 30 jours et un maximum de 7 ans (2557 jours). AWS Config supprime les données antérieures à la période de conservation que vous avez spécifiée. Si vous ne spécifiez pas de période de conservation, AWS Config continue à stocker les objets `ConfigurationItems` pendant la période par défaut de 7 ans (2 557 jours). Lorsque l'enregistrement est activé, l'état actuel de la ressource est défini lorsqu'un objet `ConfigurationItem` est enregistré et jusqu'à la prochaine modification (nouvel objet `ConfigurationItem`).

Pour comprendre le comportement de la période de conservation, observons la chronologie.

- Lorsque l'enregistrement est activé, l'état actuel d'une ressource existe toujours et ne peut pas être supprimé, quelle que soit la date d'enregistrement de l'objet `ConfigurationItem`.
- Lorsque AWS Config les enregistrements sont nouveaux`ConfigurationItems`, les précédents `ConfigurationItems` sont supprimés en fonction de la période de conservation spécifiée.

Dans la chronologie suivante, AWS Config enregistre `ConfigurationItems` aux dates suivantes. Pour les besoins de cette chronologie, aujourd'hui est représenté sous la forme du 24 mai 2018.



Le tableau suivant explique quels objets `ConfigurationItems` sont affichés sur la chronologie AWS Config en fonction de la période de conservation sélectionnée.

Période de conservation	Éléments de configuration affichés sur la chronologie	Explication
30 jours	12 décembre 2017	État actuel de la ressource démarrée le 12 décembre 2017 lorsque l'objet `ConfigurationItem` a été enregistré, valide jusqu'à aujourd'hui (24 mai 2018). Lorsque l'enregistrement est activé, l'état actuel existe toujours.
365 jours	12 décembre 2017, 12 novembre 2017 et 10 mars 2017	La période de conservation indique la date actuelle, 12 décembre 2017, et les objets `ConfigurationItems` précédents, 12 novembre 2017 et 10 mars 2017.

Période de conservation	Éléments de configuration affichés sur la chronologie	Explication
		L'objet `ConfigurationItem` pour le 10 mars 2017 s'affiche sur la chronologie, car cet état de configuration représentait l'état actuel il y a 365 jours.

Une fois que vous avez spécifié une période de rétention, AWS Config les API `ConfigurationItems` qui représentent un état antérieur à la période de rétention spécifiée ne sont plus renvoyées.

> **Note**
>
> - AWS Config Impossible de vous enregistrer `ConfigurationItems` si l'enregistrement est désactivé.
> - AWS Config Impossible de vous enregistrer `ConfigurationItems` si votre rôle IAM ne dispose pas d'autorisations suffisantes. Pour plus d'informations, consultez la section Autorisations relatives au rôle IAM attribué à AWS Config.

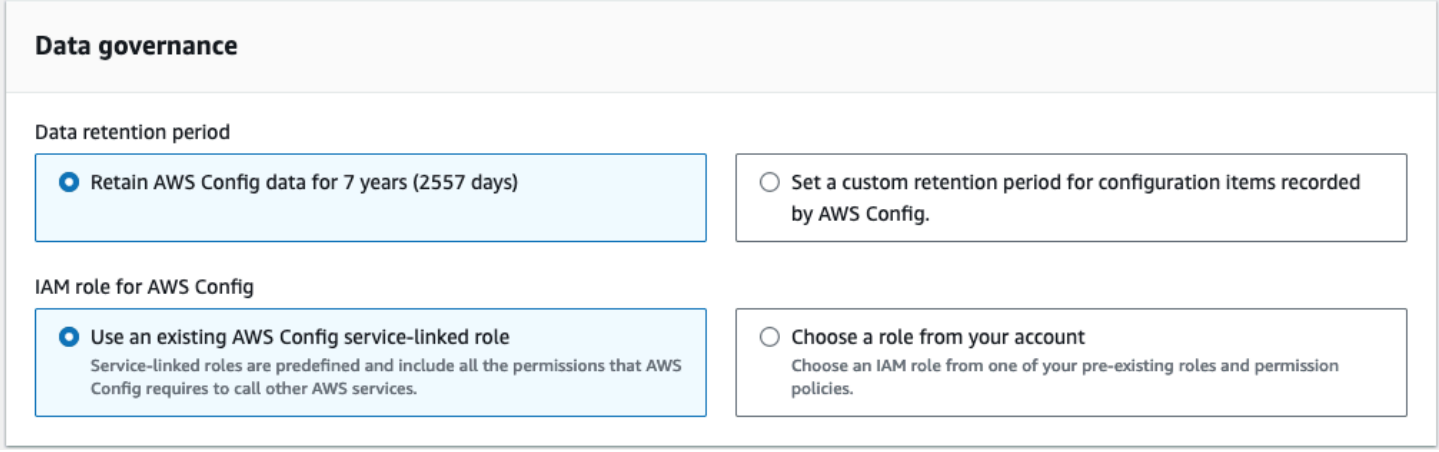
Définition de la période de conservation des données dans AWS Management Console

Dans le cas AWS Management Console où vous ne sélectionnez pas de période de conservation des données, la période par défaut est de 7 ans ou 2557 jours.

Pour définir une période de conservation des données personnalisée pour les éléments de configuration, sélectionnez la case à cocher. Vous pouvez sélectionner 1 an, 3 ans, 5 ans ou une période personnalisée. Pour une période personnalisée, entrez un nombre de jours compris entre 30 et 2 557.

L'image suivante montre où vous pouvez définir la période de conservation des données dans Data Governance. Vous pouvez accéder à la gouvernance des données sur la page Modifier les

paramètres depuis la AWS Config console en choisissant Paramètres dans la barre de navigation de gauche, puis en choisissant Modifier.



Sécurité dans AWS Config

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Config, consultez les AWS services de la section Étendue par programme de conformité et .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Config. Les rubriques suivantes expliquent comment procéder à la configuration AWS Config pour atteindre vos objectifs de sécurité et de conformité.

Rubriques

- Protection des données dans AWS Config
- Identity and Access Management pour AWS Config
- Réponse aux incidents dans AWS Config
- Validation de conformité pour AWS Config
- Résilience dans AWS Config
- Sécurité de l'infrastructure dans AWS Config
- Prévention du cas de figure de l'adjoint désorienté entre services
- Bonnes pratiques en matière de sécurité pour AWS Config

Protection des données dans AWS Config

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans AWS Config. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS Config ou autre Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans

des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement de données au repos

Les données sont chiffrées au repos à l'aide d'un chiffrement transparent côté serveur. Cela réduit la lourdeur opérationnelle et la complexité induites par la protection des données sensibles. Le chiffrement au repos vous permet de créer des applications sensibles en matière de sécurité qui sont conformes aux exigences réglementaires et de chiffrement.

Chiffrement des données en transit

Les données collectées et consultées par AWS Config se font exclusivement via un canal protégé par le protocole TLS (Transport Layer Security).

Identity and Access Management pour AWS Config

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS Config les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment AWS Config fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour AWS Config
- AWS politiques gérées pour AWS Config
- Autorisations pour le rôle IAM attribué à AWS Config
- Mise à jour du rôle IAM attribué à AWS Config
- Autorisations pour le compartiment Amazon S3 pour le canal AWS Config de diffusion
- Autorisations relatives à la clé KMS pour le canal AWS Config de distribution

- Autorisations relatives à la rubrique Amazon SNS
- Résolution des problèmes AWS Config d'identité et d'accès
- Utilisation de rôles liés à un service pour AWS Config

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez. AWS Config

Utilisateur du service : si vous utilisez le AWS Config service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS Config fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS Config, consultez Résolution des problèmes AWS Config d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AWS Config ressources de votre entreprise, vous avez probablement un accès complet à AWS Config. C'est à vous de déterminer les AWS Config fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AWS Config, voirComment AWS Config fonctionne avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à AWS Config. Pour consulter des exemples de politiques AWS Config basées sur l'identité que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS Config

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs

(IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent

des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal

(utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de

confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Config fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Config, découvrez les fonctionnalités IAM disponibles. AWS Config

Fonctionnalités IAM que vous pouvez utiliser avec AWS Config

Fonction IAM	AWS Config soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non

Fonction IAM	AWS Config soutien
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Config les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AWS Config

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou

refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour AWS Config

Pour consulter des exemples de politiques AWS Config basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Config

Politiques basées sur les ressources au sein de AWS Config

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour AWS Config

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des AWS Config actions, reportez-vous à la section Actions définies par AWS Config dans la référence d'autorisation de service.

Les actions de politique en AWS Config cours utilisent le préfixe suivant avant l'action :

```
config
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "config:Describe*"
```

Pour consulter des exemples de politiques AWS Config basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Config

Ressources politiques pour AWS Config

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de AWS Config ressources et de leurs ARN, consultez la section Ressources définies par AWS Config dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Config.

Pour consulter des exemples de politiques AWS Config basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Config

Clés de conditions de politique pour AWS Config

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de AWS Config condition, reportez-vous à la section Clés de condition pour AWS Config la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Config.

Pour consulter des exemples de politiques AWS Config basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS Config

ACL dans AWS Config

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec AWS Config

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès basé sur les attributs (ABAC) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur le balisage des ressources AWS Config , consultez Balisage de vos ressources AWS Config.

Utilisation d'informations d'identification temporaires avec AWS Config

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour AWS Config

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour AWS Config

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber AWS Config les fonctionnalités. Modifiez les rôles de service uniquement lorsque AWS Config vous recevez des instructions à cet effet.

Rôles liés à un service pour AWS Config

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles AWS Config liés à un service, consultez. Utilisation de rôles liés à un service pour AWS Config

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour AWS Config

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources AWS Config . Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Config, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS Config dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif
- Utilisation de la console AWS Config
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accès en lecture seule à AWS Config
- Accès complet à AWS Config
- Autorisations prises en charge au niveau des ressources pour les actions d'API de AWS Config règles
- Autorisations au niveau des ressources prises en charge pour l'agrégation de données multi-région et multi-compte

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS Config des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l‘URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l‘utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisation de la console AWS Config

Pour accéder à la AWS Config console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails AWS Config des ressources de votre Compte AWS. Si vous créez une stratégie basée sur l’identité qui est plus restrictive que l’ensemble minimum d’autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la AWS Config console, associez également la politique AWS Config `AWSConfigUserAccess` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Vous devez autoriser les utilisateurs à interagir avec AWS Config. Pour les utilisateurs qui ont besoin d'un accès complet à AWS Config, utilisez la politique Accès complet à la AWS Config gestion.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès en lecture seule à AWS Config

L'exemple suivant montre une politique AWS gérée `AWSConfigUserAccess` qui accorde un accès en lecture seule à. AWS Config

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
```

```
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

Dans les déclarations de politique, l'élément `Effect` spécifie si les actions sont autorisées ou refusées. L'élément `Action` répertorie les actions spécifiques que l'utilisateur est autorisé à effectuer. L'élément `Resource` répertorie les ressources AWS sur lesquelles l'utilisateur est autorisé à effectuer ces actions. Pour les politiques qui contrôlent l'accès aux AWS Config actions, l'`Resource`élément est toujours défini sur`*`, un caractère générique qui signifie « toutes les ressources ».

Les valeurs dans l'élément `Action` correspondent aux API prises en charge par les services. Les actions sont précédées de `config:` pour indiquer qu'elles font référence à des actions AWS Config . Vous pouvez utiliser le caractère générique `*` dans l'élément `Action`, comme dans les exemples suivants :

- `"Action": ["config:*ConfigurationRecorder"]`

  Cela autorise toutes les AWS Config actions qui se terminent par ConfigurationRecorder "" (`StartConfigurationRecorder`,`StopConfigurationRecorder`).
- `"Action": ["config:*"]`

  Cela permet toutes les AWS Config actions, mais pas les actions pour les autres AWS services.
- `"Action": ["*"]`

  Cela permet toutes les AWS actions. Cette autorisation convient à un utilisateur qui agit en tant qu' AWS administrateur de votre compte.

La stratégie en lecture seule n'accorde pas l'autorisation à l'utilisateur pour les actions `StartConfigurationRecorder`, `StopConfigurationRecorder` et

`DeleteConfigurationRecorder`. Les utilisateurs disposant de cette stratégie ne sont pas autorisés à démarrer, arrêter ou supprimer l'enregistreur de configuration. Pour la liste des AWS Config actions, consultez la référence de AWS Config l'API.

Accès complet à AWS Config

L'exemple suivant montre une politique qui accorde un accès complet à AWS Config. Il accorde aux utilisateurs l'autorisation d'effectuer toutes les AWS Config actions. Ils sont aussi autorisés à gérer les fichiers dans des compartiments Amazon S3, ainsi que les rubriques Amazon SNS du compte auquel ils sont associés.

> **Important**
>
> Cette politique accorde des autorisations étendues. Avant d'accorder un accès complet, commencez avec un ensemble d'autorisations minimum et accordez-en d'autres si nécessaire. Cette méthode est plus sûre que de commencer avec des autorisations trop permissives et d'essayer de les restreindre plus tard.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
```

```
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

Autorisations prises en charge au niveau des ressources pour les actions d'API de AWS Config règles

Les autorisations au niveau des ressources font référence à la capacité de spécifier les ressources sur lesquelles les utilisateurs sont autorisés à effectuer des actions. AWS Config prend en charge les autorisations au niveau des ressources pour certaines actions d'API de AWS Config règles. Cela signifie que pour certaines actions de AWS Config règles, vous pouvez contrôler les conditions dans lesquelles les utilisateurs sont autorisés à utiliser ces actions. Ces conditions peuvent être des

actions qui doivent être réalisées, ou des ressources spécifiques que les utilisateurs sont autorisés à utiliser.

Le tableau suivant décrit les actions d'API de AWS Config règles qui prennent actuellement en charge les autorisations au niveau des ressources. Il décrit également les ressources prises en charge et leurs ARN pour chaque action. Lorsque vous spécifiez un ARN, vous pouvez utiliser le caractère générique * dans vos chemins ; par exemple, quand vous ne voulez ou ne pouvez pas spécifier des ID de ressource exacts.

> **Important**
>
> Si une action d'API de AWS Config règle n'est pas répertoriée dans ce tableau, cela signifie qu'elle ne prend pas en charge les autorisations au niveau des ressources. Si une action de AWS Config règle ne prend pas en charge les autorisations au niveau des ressources, vous pouvez autoriser les utilisateurs à utiliser l'action, mais vous devez spécifier un * pour l'élément ressource de votre déclaration de politique.

Action d'API	Ressources
DeleteConfigRègle	Règle de configuration arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DeleteEvaluationRésultats	Règle de configuration arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeCompliance ByConfigRègle	Règle de configuration arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeConfigRuleEvaluatio nÉtat	Règle de configuration arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
GetComplianceDetailsByConfi gRule	Règle de configuration arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*

Action d'API	Ressources
PutConfigRègle	Règle de configuration arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Règle de configuration arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutRemediationConfigurations	Configuration de la correction arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationConfigurations	Configuration de la correction arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationConfiguration	Configuration de la correction arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
PutRemediationExceptions	Configuration de la correction arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationExceptions	Configuration de la correction arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

Action d'API	Ressources
DeleteRemediationExceptions	Configuration de la correction arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

Par exemple, vous voulez autoriser l'accès en lecture et refuser l'accès en écriture à des règles spécifiques à des utilisateurs spécifiques.

Dans la première politique, vous autorisez les actions de lecture des AWS Config règles, par exemple `DescribeConfigRuleEvaluationStatus` sur les règles spécifiées.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

Dans la seconde politique, vous refusez les actions d'écriture de AWS Config règles sur la règle spécifique.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

Avec les autorisations au niveau des ressources, vous pouvez autoriser l'accès en lecture et refuser l'accès en écriture pour effectuer des actions spécifiques sur les actions de l'API de AWS Config règles.

Autorisations au niveau des ressources prises en charge pour l'agrégation de données multi-région et multi-compte

Vous pouvez utiliser des autorisations au niveau des ressources pour contrôler la capacité d'un utilisateur à effectuer des actions spécifiques sur des regroupements de données de plusieurs comptes et plusieurs régions. Les AWS Config `Aggregator` API suivantes prennent en charge les autorisations au niveau des ressources :

- BatchGetAggregateResourceConfig
- DeleteConfigurationAgrégateur
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesÉtat
- GetAggregateComplianceDetailsByConfigRègle
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceComtes
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources

- PutConfigurationAgrégateur
- SelectAggregateResourceConfig

Vous pouvez par exemple restreindre l'accès aux données des ressources pour des utilisateurs spécifiques en créant deux agrégateurs `AccessibleAggregator` et `InAccessibleAggregator` et en attachant une politique IAM qui autorise l'accès à `AccessibleAggregator` en refusant l'accès à `InAccessibleAggregator`.

Politique IAM pour AccessibleAggregator

Cette politique vous permet d'autoriser l'accès aux actions de l'agrégateur pris en charge pour l'Amazon Resource Name (ARN) AWS Config que vous spécifiez. Dans cet exemple, l' AWS Config ARN est`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

Politique IAM pour InAccessibleAggregator

Dans cette politique, vous refusez l'accès aux actions d'agrégation prises en charge pour l' AWS Config ARN que vous spécifiez. Dans cet exemple, l' AWS Config ARN est`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

Si un utilisateur du groupe de développeurs essaie d'effectuer l'une de ces actions sur l' AWS Config ARN que vous avez spécifié, il obtiendra une exception de refus d'accès.

Vérification des autorisations d'accès des utilisateurs

Pour afficher les agrégateurs que vous avez créés, exécutez la AWS CLI commande suivante :

```
aws configservice describe-configuration-aggregators
```

Une fois la commande exécutée, vous pourrez consulter les détails de tous les agrégateurs associés à votre compte. Dans cet exemple, il s'agit des agrégateurs `AccessibleAggregator` et `InAccessibleAggregator` :

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> Pour `account-aggregation-sources`, entrez une liste d'ID de compte AWS séparés par des virgules, pour lesquels vous souhaitez regrouper les données. Placez les ID de compte entre crochets avec une mise en échappement (par exemple, `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).

Attachez la politique IAM suivante pour refuser l'accès à `InAccessibleAggregator` ou à l'agrégateur auquel vous souhaitez refuser l'accès.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

Vous pouvez ensuite confirmer que la politique IAM fonctionne pour limiter l'accès aux règles pour un agrégateur spécifique :

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

La commande doit renvoyer une exception d'accès rejeté :

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS politiques gérées pour AWS Config

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSConfigServiceRolePolicy

AWS Config utilise le rôle lié au service nommé AWSServiceRoleForConfigpour appeler d'autres AWS services en votre nom. Lorsque vous utilisez le AWS Management Console pour le configurer

AWS Config, ce reflex est automatiquement créé AWS Config si vous sélectionnez l'option permettant d'utiliser le AWS Config reflex au lieu de votre propre rôle de service AWS Identity and Access Management (IAM).

Le SLR AWSServiceRoleForConfig contient la politique gérée `AWSConfigServiceRolePolicy`. Cette politique gérée contient des autorisations en lecture seule et en écriture uniquement pour les ressources et des autorisations en lecture seule pour les AWS Config ressources des autres services pris en charge. AWS Config Pour plus d'informations, consultez Types de ressource pris en charge et Utilisation de rôles liés à un service pour AWS Config.

Consultez la politique : AWSConfigServiceRolePolicy.

AWS politique gérée : AWS_ConfigRole

Pour enregistrer vos configurations de AWS ressources, vous AWS Config devez disposer des autorisations IAM pour obtenir les détails de configuration de vos ressources. Si vous souhaitez créer un rôle IAM pour AWS Config, vous pouvez utiliser la politique gérée `AWS_ConfigRole` et l'attacher à votre rôle IAM.

Cette politique IAM est mise à jour chaque fois que la prise en charge d'un type de AWS ressource est AWS Config ajoutée. Cela signifie qu'il AWS Config continuera à disposer des autorisations requises pour enregistrer les données de configuration des types de ressources pris en charge tant que cette politique gérée sera attachée au ConfigRole rôle AWS_. Pour plus d'informations, consultez Types de ressource pris en charge et Autorisations pour le rôle IAM attribué à AWS Config.

Consultez la politique : AWS_ ConfigRole.

AWS politique gérée : AWSConfigUserAccess

Cette politique IAM fournit un accès à l'utilisation AWS Config, y compris la recherche par balises sur les ressources et la lecture de toutes les balises. Cela ne donne pas l'autorisation de configurer AWS Config, ce qui nécessite des privilèges administratifs.

Consultez la politique : AWSConfigUserAccess.

AWS politique gérée : ConfigConformsServiceRolePolicy

Le déploiement et la gestion des packs de conformité AWS Config nécessitent des autorisations IAM et certaines autorisations d'autres AWS services. Ils vous permettent de déployer et de gérer des

packs de conformité avec toutes les fonctionnalités et sont mis à jour chaque fois que de nouvelles AWS Config fonctionnalités sont ajoutées aux packs de conformité. Pour plus d'informations sur les packs de conformité, consultez Packs de conformité.

Consultez la politique : ConfigConformsServiceRolePolitique.

AWS politique gérée : AWSConfigRulesExecutionRole

Pour déployer AWS des règles Lambda personnalisées, des autorisations AWS Config IAM et certaines autorisations d'autres services sont nécessaires. AWS Ils permettent aux AWS Lambda fonctions d'accéder à l' AWS Config API et aux instantanés de configuration AWS Config fournis régulièrement à Amazon S3. Cet accès est requis par les fonctions qui évaluent les modifications de configuration pour les règles Lambda AWS personnalisées et est mis à jour chaque fois que de nouvelles fonctionnalités sont AWS Config ajoutées. Pour plus d'informations sur les règles Lambda AWS personnalisées, voir Création de règles AWS Config Lambda personnalisées et composants d'une règle. AWS Config Pour plus d'informations sur les instantanés de configuration, consultez Concepts | Instantané de configuration. Pour plus d'informations sur la livraison des instantanés de configuration, consultez Gestion du canal de livraison.

Consultez la politique : AWSConfigRulesExecutionRole.

AWS politique gérée : AWSConfigMultiAccountSetupPolicy

Le déploiement, la mise à jour et la suppression centralisés des AWS Config règles et des packs de conformité sur les comptes des membres d'une organisation AWS Config nécessitent des autorisations IAM et certaines autorisations d'autres AWS services. AWS Organizations Cette politique gérée est mise à jour chaque fois qu' AWS Config une nouvelle fonctionnalité est ajoutée pour la configuration de plusieurs comptes. Pour plus d'informations, consultez les sections Gestion des AWS Config règles pour tous les comptes de votre organisation et Gestion des packs de conformité pour tous les comptes de votre organisation.

Consultez la politique : AWSConfigMultiAccountSetupPolicy.

AWS politique gérée : AWSConfigRoleForOrganizations

AWS Config Pour autoriser l'appel d' AWS Organizations API en lecture seule, des autorisations AWS Config IAM et certaines autorisations d'autres services sont nécessaires. AWS Cette politique gérée est mise à jour chaque fois qu' AWS Config une nouvelle fonctionnalité est ajoutée pour la configuration de plusieurs comptes. Pour plus d'informations, consultez les sections Gestion des

AWS Config règles pour tous les comptes de votre organisation et Gestion des packs de conformité pour tous les comptes de votre organisation.

Consultez la politique : AWSConfigRoleForOrganizations.

AWS politique gérée : AWSConfigRemediationServiceRolePolicy

AWS Config Pour autoriser la correction `NON_COMPLIANT` des ressources en votre nom, vous devez AWS Config disposer d'autorisations IAM et de certaines autorisations accordées par d'autres AWS services. Cette politique gérée est mise à jour chaque fois qu' AWS Config une nouvelle fonctionnalité de correction est ajoutée. Pour plus d'informations sur la correction, voir Corriger les ressources non conformes à l'aide de règles. AWS Config Pour plus d'informations sur les conditions à l'origine des résultats AWS Config d'évaluation possibles, voir Concepts | AWS Config Règles.

Consultez la politique : AWSConfigRemediationServiceRolePolicy.

AWS Config mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Config depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AWS Config document.

Modification	Description	Date
AWS_ConfigRole – Ajout de elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Elastic File System (Amazon EFS), Amazon Redshift et. Gestionnaire de systèmes AWS pour SAP	17 juin 2024
AWSConfigServiceRolePolicy – Ajout de elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Elastic File System (Amazon	17 juin 2024

Modification	Description	Date
	EFS), Amazon Redshift et. Gestionnaire de systèmes AWS pour SAP	

Modification	Description	Date
AWS_ConfigRole – Ajout de "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments,	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Service pour Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, Amazon AWS Glue FSx ElastiCache, (IAM) AWS Identity and Access Management ,,, Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon et Amazon Simple Notification Service (SageMakerAmazon SNS).	22 février 2024

Modification	Description	Date
" and "sns:GetSMSSand boxAccountStatus"		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments,	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Service pour Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, Amazon AWS Glue FSx ElastiCache, (IAM) AWS Identity and Access Management ,,, Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon et Amazon Simple Notification Service (SageMakerAmazon SNS).	22 février 2024

Modification	Description	Date
" and "sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess— AWS Config commence à suivre les modifications apportées à cette politique AWS gérée	Cette politique fournit un accès à l'utilisation AWS Config, y compris la recherche par balises sur les ressources et la lecture de toutes les balises. Cela ne donne pas l'autorisation de configurer AWS Config, ce qui nécessite des privilèges administratifs.	22 février 2024
AWS_ConfigRole – Ajout de "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management(Amazon MSK) AWS Organizations, Amazon Logs et CloudWatch Amazon Simple Storage Service (Amazon S3).	5 décembre 2023

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management(Amazon MSK) AWS Organizations, Amazon Logs et CloudWatch Amazon Simple Storage Service (Amazon S3).	5 décembre 2023

Modification	Description	Date
AWS_ConfigRole – Ajout de "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, AWS Mainframe Modernization Amazon MemoryDB pour Redis, Amazon, Amazon, QuickSight Amazon AWS Organizations Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 et. AWS Service Catalog AWS Transfer Family	17 novembre 2023

Modification	Description	Date
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

Modification	Description	Date
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole – Ajout de "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Cette politique ajoute désormais des identificateurs de sécurité (SID) pour `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` et `AWSConfigSLRApiGatewayStatementID` .	17 novembre 2023

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, AWS Mainframe Modernization Amazon MemoryDB pour Redis, Amazon, Amazon, QuickSight Amazon AWS Organizations Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 et. AWS Service Catalog AWS Transfer Family	17 novembre 2023

Modification	Description	Date
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

Modification	Description	Date
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy – Ajout de "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Cette politique ajoute désormais des identificateurs de sécurité (SID) pour `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` et `AWSConfigSLRApiGatewayStatementID` .	17 novembre 2023

Modification	Description	Date
AWS_ConfigRole – Ajout de "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Private CA AWS App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon Evidently , CloudWatch Amazon Managed Grafana, Amazon, Amazon, GuardDuty Amazon AWS IoT AWS IoT TwinMaker Inspector,,,, Amazon Managed Streaming for Apache Kafka (Amazon AWS Lambda MSK AWS Network Manager),,, et Amazon. AWS Organizations SageMaker	4 octobre 2023

Modification	Description	Date
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Private CA AWS App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon Evidently , CloudWatch Amazon Managed Grafana, Amazon, Amazon, GuardDuty Amazon AWS IoT AWS IoT TwinMaker Inspector,,,, Amazon Managed Streaming for Apache Kafka (Amazon AWS Lambda MSK AWS Network Manager),,, et Amazon. AWS Organizations SageMaker	4 octobre 2023

Modification	Description	Date
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy— Supprimer "ssm:GetParameter"	Cette politique supprime désormais les autorisations pour AWS Systems Manager (Systems Manager).	6 septembre 2023

Modification	Description	Date
AWS_ConfigRole – Ajout de "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets",	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon AWS App Mesh AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact AWS CodeBuild, Amazon AWS Identity and Access Management (IAM) AWS Glue, Amazon Inspector GuardDuty,,,, Amazon Managed Streaming pour Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Macie,,,, ,,,, Amazon Route 53 AWS Elemental MediaConnect AWS Network Manager AWS Organizations Explorateur de ressources AWS, Amazon Simple Storage Service (Amazon S3) et Amazon Simple Notification Service (Amazon SNS) Simple Notification (Amazon SNS).	28 juillet 2023

Modification	Description	Date
"macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets", "m	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS App Mesh Amazon AppStream 2.0, Amazon AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact AWS CodeBuild, Amazon AWS Identity and Access Management (IAM) AWS Glue, Amazon Inspector GuardDuty,,,, Amazon Managed Streaming pour Apache Kafka AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Macie,,,,, Amazon Route 53 AWS Elemental MediaConnect, Amazon Simple Storage Service (Amazon S3) AWS Network Manager AWS Organizations Explorateur de ressources AWS, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon (SNS) et Amazon EC2 Systems Manager (SSM).	28 juillet 2023

Modification	Description	Date
acie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

Modification	Description	Date
AWS_ConfigRole – Ajout de "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Amplify Amazon Connect AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena,,,,,, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon EC2) CodeGuru, Amazon CloudWatch Evidently, Amazon Forecast,,, (IAM), Amazon Managed Streaming pour Apache Kafka Managed for Apache (AWS Ground Station AWS Identity and Access Management Amazon MSK) AWS IoT Greengrass, Amazon Lightsail, Amazon Logs, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon AWS Organizations CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC), Amazon Personalize QuickSight, Amazon, AWS Migration Hub Refactor Spaces Amazon Simple Storage Service (Amazon S3),	13 juin 2023

Modification	Description	Date
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "org	Amazon,. SageMaker AWS Transfer Family	

Modification	Description	Date
anizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Amplify Amazon Connect AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena,,,,,, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon EC2) CodeGuru, Amazon CloudWatch Evidently, Amazon Forecast,,, (IAM), Amazon Managed Streaming pour Apache Kafka Managed for Apache (AWS Ground Station AWS Identity and Access Management Amazon MSK) AWS IoT Greengrass, Amazon Lightsail, Amazon Logs, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon AWS Organizations CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC), Amazon Personalize QuickSight, Amazon, AWS Migration Hub Refactor Spaces Amazon Simple Storage Service (Amazon S3),	13 juin 2023

Modification	Description	Date
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAcc	Amazon,. SageMaker AWS Transfer Family	

Modification	Description	Date
ountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour AWS Amplify AWS App Mesh AWS App Runner, CloudFront, Amazon AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, SageMaker Amazon, AWS Transfer Family Amazon Pinpoint, Resilience Hub AWS , Amazon CloudWatch, AWS Directory Service et. AWS Migration Hub AWS WAF	13 avril 2023

Modification	Description	Date
ion, macie2:GetClassificatio nExportConfiguration, macie2 :GetCustomDataIdentifier, ma cie2:GetFindingsPublication Configuration, macie2:ListCu stomDataIdentifiers, mobiletar geting:GetEmailChannel, refa ctor-spaces:GetEnvironment, refactor-spaces:ListEnviron ments, resiliencehub:ListTag sForResource, route53:G etDNSSEC, sagemaker :DescribeDomain, sagemaker :DescribeModelBiasJobDefini tion, sagemaker:Des cribeModelQualityJobDefinit ion, sagemaker:DescribePipel ine, sagemaker:Describe Project, sagemaker:ListDomai ns, sagemaker:ListMode lBiasJobDefinitions, sagemak er:ListModelQualityJobDefin itions, sagemaker:ListPipe lines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificat e, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLogging Configurations		

Modification	Description	Date
AWS_ConfigRole – Ajout de amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificati	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour AWS Amplify AWS App Mesh AWS App Runner, CloudFront, Amazon AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, SageMaker Amazon, AWS Transfer Family Amazon Pinpoint, Resilience Hub AWS , Amazon CloudWatch, AWS Directory Service et. AWS Migration Hub AWS WAF	13 avril 2023

Modification	Description	Date
onExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAML	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour Amazon AppFlow AWS App Runner, Amazon AppStream 2.0, Amazon CloudFront, CloudWatch, AWS CodeArtifact AWS CodeCommit, Amazon CloudWatch Evidently AWS Device Farm, Amazon Forecast, AWS Identity and Access Management (IAM) AWS Ground Station, AWS IoT Amazon MemoryDB pour Redis, Amazon Pinpoint, ,, Amazon AWS Network Manager Relational Database AWS Panorama Service (Amazon RDS), Amazon Redshift et Amazon. SageMaker	30 mars 2023

Modification	Description	Date
Provider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Modification	Description	Date
AWS_ConfigRole – Ajout de appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundsta	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour Amazon AppFlow AWS App Runner, Amazon AppStream 2.0 AWS CloudFormation, Amazon CloudFront,,, CloudWatch, AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidently, CloudWatch Amazon Forecast, (AWS IoT IAM), AWS Ground Station Amazon AWS Identity and Access Management MemoryDB pour Redis, Amazon Pinpoint AWS Network Manager,, AWS Panorama Amazon Relational Database Service (Amazon RDS), Amazon Redshift et Amazon. SageMaker	30 mars 2023

Modification	Description	Date
tion:GetConfig, groundst ation:ListConfigs, groundst ation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, i am:ListAccessKeys, iam:List Groups, iam:ListInstancePro files, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAM LProviders, iot:DescribeFle etMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobile targeting:GetApp, mobiletar geting:GetCampaigns, networ kmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, p anorama:ListNodes, rds:Desc ribeDBProxyEndpoints, redsh ift:DescribeScheduledActions, sagemaker:DescribeAppIma geConfig, sagemaker:Describ eImage, sagemaker:DescribeI mageVersion, sagem aker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Modification	Description	Date
AWSConfigRulesExecutionRole— AWS Config commence à suivre les modifications apportées à cette politique AWS gérée	Cette politique permet aux AWS Lambda fonctions d'accéder à l' AWS Config API et aux instantanés de configuration AWS Config fournis régulièrement à Amazon S3. Cet accès est requis par les fonctions qui évaluent les modifications de configuration pour les AWS règles Lambda personnalisées.	7 mars 2023
AWSConfigRoleForOrganizations— AWS Config commence à suivre les modifications apportées à cette politique AWS gérée	Cette politique permet d' AWS Config appeler des API en lecture seule AWS Organizations .	7 mars 2023
AWSConfigRemediationServiceRolePolicy— AWS Config commence à suivre les modifications apportées à cette politique AWS gérée	Cette politique permet AWS Config de corriger les `NON_COMPLIANT` ressources en votre nom.	7 mars 2023
AWSConfigServiceRolePolicy – Ajout de auditmanager:GetAccountStatus	Cette politique autorise désormais le renvoi de l'état d'enregistrement d'un compte dans AWS Audit Manager.	3 mars 2023
AWS_ConfigRole – Ajout de auditmanager:GetAccountStatus	Cette politique autorise désormais le renvoi de l'état d'enregistrement d'un compte dans AWS Audit Manager.	3 mars 2023

Modification	Description	Date
AWSConfigMultiAccountSetupPolicy— AWS Config commence à suivre les modifications apportées à cette politique AWS gérée	Cette politique permet d' AWS Config appeler AWS des services et de déployer AWS Config des ressources au sein d'une organisation avec AWS Organizations.	27 février 2023

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefarm:L	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Route 53 Application Recovery Controller AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon AWS Identity and Access Management Pinpoint (IAM), Amazon et Amazon Logs. GuardDuty CloudWatch	1er février 2023

Modification	Description	Date
istTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Modification	Description	Date
AWS_ConfigRole – Ajout de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Route 53 Application Recovery Controller AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon AWS Identity and Access Management Pinpoint (IAM), Amazon et Amazon Logs. GuardDuty CloudWatch	1er février 2023

Modification	Description	Date
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – Mise à jour de config:DescribeConfigRules	À titre de bonne pratique de sécurité, cette politique supprime désormais les autorisations étendues au niveau des ressources pour `config:DescribeConfigRules` .	12 janvier 2023

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Service pour Prometheus AWS Audit Manager,,, AWS Device Farm,AWS DMS() AWS Database Migration Service AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2 AWS Glue) AWS IoT,, Amazon Lightsail AWS Elemental MediaPackage,,, Amazon, Amazon, Amazon Route 53 Application Recovery Controller AWS Network Manager QuickSight, AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) et Amazon Timestream Am.	15 décembre 2022

Modification	Description	Date
Resource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modification	Description	Date
AWS_ConfigRole – Ajout de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Service pour Prometheus AWS Audit Manager,,, AWS Device Farm,AWS DMS() AWS Database Migration Service AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2 AWS Glue) AWS IoT,, Amazon Lightsail AWS Elemental MediaPackage,,, Amazon, Amazon, Amazon Route 53 Application Recovery Controller AWS Network Manager QuickSight, AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) et Amazon Timestream Am.	15 décembre 2022

Modification	Description	Date
Resource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de cloudformation:ListStackResources and cloudformation:ListStacks	Cette politique accorde désormais l'autorisation de renvoyer des descriptions de toutes les ressources d'une AWS CloudFormation pile spécifiée et de renvoyer les informations récapitulatives pour les piles dont le statut correspond à celui spécifiéStackStatusFilter.	7 novembre 2022
AWS_ConfigRole – Ajout de cloudformation:ListStackResources and cloudformation:ListStacks	Cette politique accorde désormais l'autorisation de renvoyer des descriptions de toutes les ressources d'une AWS CloudFormation pile spécifiée et de renvoyer les informations récapitulatives pour les piles dont le statut correspond à celui spécifiéStackStatusFilter.	7 novembre 2022

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersi	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Certificate Manager Amazon Managed Workflows pour Apache Airflow AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect, CloudWatch Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx EventBridge, AWS Fault Injection Service Amazon, Amazon GameLift Location Service, Amazon AWS IoT Lex, Amazon Lightsail, Amazon Pinpoint,,,, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3), et. AWS Security Token Service	19 octobre 2022

Modification	Description	Date
ons, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsite		

Modification	Description	Date
wise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage		

Modification	Description	Date
, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modification	Description	Date
AWS_ConfigRole – Ajout de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersions, databrew:ListRulesets,	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Certificate Manager Amazon Managed Workflows pour Apache Airflow AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect, CloudWatch Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx EventBridge, AWS Fault Injection Service Amazon, Amazon GameLift Location Service, Amazon AWS IoT Lex, Amazon Lightsail, Amazon Pinpoint,,,, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3), et. AWS Security Token Service	19 octobre 2022

Modification	Description	Date
databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsit		

Modification	Description	Date
ewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage, panorama:Describe		

Modification	Description	Date
PackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de Glue::GetTable	Cette politique accorde désormais l'autorisation de récupérer la définition de AWS Glue table dans un catalogue de données pour une table spécifiée.	14 septembre 2022
AWS_ConfigRole – Ajout de Glue::GetTable	Cette politique accorde désormais l'autorisation de récupérer la définition de AWS Glue table dans un catalogue de données pour une table spécifiée.	14 septembre 2022

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirr	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR EventBridge, Amazon, Amazon Schemas, Amazon GameLift Fraud Detector Detector, EventBridge Amazon Amazon FinSpace, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service pour Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon, Amazon Route 53 Resolver contrôleu	7 septembre 2022

Modification	Description	Date
orFilters, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, game	r de restauration d'applications QuickSight Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager AWS Resilience Hub, AWS Signer, et AWS Transfer Family.	

Modification	Description	Date
lift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:Desc		

Modification	Description	Date
ribeSecurityProfile, iot:Get Policy, iot:GetTopicRule, iot :GetTopicRuleDestination, iot:ListCertificates, iot:List Dimensions, iot:ListPolicies , iot:ListRoleAliases, iot:Li stSecurityProfiles, iot:List SecurityProfilesForTarget, i ot:ListTagsForResource, iot: ListTargetsForSecurityProfi le, iot:ListTopicRuleDestina tions, iot:ListTopicRules, io t:ListV2LoggingLevels, iot:V alidateSecurityProfileBehav iors, iotanalytics:DescribeC hannel, iotanalytics:Describ eDataset, iotanalytics:Descr ibeDatastore, iotanalytics:D escribePipeline, iotanalytic s:ListChannels, iotanalytics :ListDatasets, iotanalytics: ListDatastores, iotanalytics :ListPipelines, iotanalytics :ListTagsForResource, ioteve nts:DescribeAlarmModel, iote vents:DescribeDetectorModel , iotevents:DescribeInput, io tevents:ListAlarmModels, iot events:ListDetectorModels, i otevents:ListInputs, ioteven ts:ListTagsForResource, iots itewise:DescribeAccessPolic y, iotsitewise:DescribeAsset , iotsitewise:ListAccessPoli cies, iotsitewise:ListAssets		

Modification	Description	Date
, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:Ge		

Modification	Description	Date
tInstance, lightsail:GetInst ances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, l ightsail:GetLoadBalancers, l ightsail:GetLoadBalancerTls Certificates, lightsail:GetS taticIp, lightsail:GetStaticIps, lookoutequipment:Descri beInferenceScheduler, lookoutequipment:ListTag sForResource, lookoutmetrics :DescribeAlert, lookoutmetri cs:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, l ookoutmetrics:ListAnomalyDe tectors, lookoutmetrics:List MetricSets, lookoutmetrics:L istTagsForResource, lookoutv ision:DescribeProject, looko utvision:ListProjects, manag edblockchain:GetMember, managedblockchain:GetN etwork, managedbloc kchain:GetNode, man agedblockchain:ListInvitati ons, managedblockch ain:ListMembers, ma nagedblockchain:ListNodes, mediapackage-vod:De scribePackagingGroup, mediapackage-vod:ListPac kagingGroups, media package-vod:ListTagsForReso urce, mobiletargeting:GetInA ppTemplate, mobiletargeting:		

Modification	Description	Date
ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies,		

Modification	Description	Date
route53-recovery-readiness: GetCell, route53-recovery-re adiness:GetReadinessCheck, route53-recovery-readiness:G etRecoveryGroup, route53- recovery-readiness:Ge tResourceSet, route53- recovery-readiness:ListC ells, route53-recovery-readi ness:ListReadinessChecks, route53-recovery-readiness:Li stRecoveryGroups, route53- recovery-readiness:ListResour ceSets, route53resolver:GetF irewallDomainList, route53re solver:GetFirewallRuleGroup , route53resolver:GetFirewal lRuleGroupAssociation, route53resolver:GetReso lverQueryLogConfig, route53r esolver:ListFirewallDomainL ists, route53resolver:ListFi rewallDomains, route53resolv er:ListFirewallRuleGroupAss ociations, route53resolver:L istFirewallRuleGroups, route53resolver:ListFir ewallRules, route53resolver: ListResolverQueryLogConfigs , rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, ru m:ListTagsForResource, s3- outposts:GetAccessPoint, s3-outposts:GetAccessPo		

Modification	Description	Date
intPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUs		

Modification	Description	Date
er, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Modification	Description	Date
AWS_ConfigRole – Ajout de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets,	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR EventBridge, Amazon, Amazon Schemas, Amazon GameLift Fraud Detector Detector, EventBridge Amazon Amazon FinSpace, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service pour Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon, Amazon Route 53 Resolver contrôleu	7 septembre 2022

Modification	Description	Date
ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttributes, gamel	r de restauration d'applications QuickSight Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker, AWS Lake Formation AWS License Manager, AWS Resilience Hub, AWS Signer, et AWS Transfer Family	

Modification	Description	Date
ift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination		

Modification	Description	Date
, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwi		

Modification	Description	Date
nmaker:ListEntities, iottwin maker:ListScenes, iottwinmak er:ListTagsForResource, iott winmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfigura tion, ivs:GetStreamKey, ivs:ListChannels, ivs:Li stPlaybackKeyPairs, ivs:List RecordingConfigurations, ivs:ListStreamKeys, iv s:ListTagsForResource, kines isanalytics:ListApplications, lakeformation:DescribeRes ource, lakeformation:GetData LakeSettings, lakeformation: ListPermissions, lakeformati on:ListResources, lex:Descri beBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:List BotLocales, lex:ListBots, lex :ListTagsForResource, licens e-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLice nses, license-manager:ListRe ceivedGrants, lightsail:GetA larms, lightsail:GetBuckets, lightsail:GetCertificates, l ightsail:GetDisk, lightsail: GetDisks, lightsail:GetInsta nce, lightsail:GetInstances, lightsail:GetKeyPair, lights		

Modification	Description	Date
ail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile,		

Modification	Description	Date
nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetRead		

Modification	Description	Date
inessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetL		

Modification	Description	Date
ifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:		

Modification	Description	Date
ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Route 53 Application Recovery Controller AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon AWS Identity and Access Management Pinpoint (IAM), Amazon et Amazon Logs. GuardDuty CloudWatch	1er février 2023

Modification	Description	Date
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Modification	Description	Date
AWS_ConfigRole – Ajout de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Workflows pour Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Route 53 Application Recovery Controller AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon AWS Identity and Access Management Pinpoint (IAM), Amazon et Amazon Logs. GuardDuty CloudWatch	1er février 2023

Modification	Description	Date
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – Mise à jour de config:DescribeConfigRules	À titre de bonne pratique de sécurité, cette politique supprime désormais les autorisations étendues au niveau des ressources pour `config:DescribeConfigRules` .	12 janvier 2023

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Service pour Prometheus AWS Audit Manager,,, AWS Device Farm,AWS DMS() AWS Database Migration Service AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2 AWS Glue) AWS IoT,, Amazon Lightsail AWS Elemental MediaPackage,,, Amazon, Amazon, Amazon Route 53 Application Recovery Controller AWS Network Manager QuickSight, AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) et Amazon Timestream Am.	15 décembre 2022

Modification	Description	Date
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modification	Description	Date
AWS_ConfigRole – Ajout de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Managed Service pour Prometheus AWS Audit Manager,,, AWS Device Farm,AWS DMS() AWS Database Migration Service AWS Directory Service, Amazon Elastic Compute Cloud (Amazon EC2 AWS Glue) AWS IoT,, Amazon Lightsail AWS Elemental MediaPackage,,, Amazon, Amazon, Amazon Route 53 Application Recovery Controller AWS Network Manager QuickSight, AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) et Amazon Timestream Am.	15 décembre 2022

Modification	Description	Date
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de cloudformation:ListStackResources and cloudformation:ListStacks	Cette politique accorde désormais l'autorisation de renvoyer des descriptions de toutes les ressources d'une AWS CloudFormation pile spécifiée et de renvoyer les informations récapitulatives pour les piles dont le statut correspond à celui spécifiéStackStatusFilter.	7 novembre 2022
AWS_ConfigRole – Ajout de cloudformation:ListStackResources and cloudformation:ListStacks	Cette politique accorde désormais l'autorisation de renvoyer des descriptions de toutes les ressources d'une AWS CloudFormation pile spécifiée et de renvoyer les informations récapitulatives pour les piles dont le statut correspond à celui spécifiéStackStatusFilter.	7 novembre 2022

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Certificate Manager Amazon Managed Workflows pour Apache Airflow AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect, CloudWatch Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx EventBridge, AWS Fault Injection Service Amazon, Amazon GameLift Location Service, Amazon AWS IoT Lex, Amazon Lightsail, Amazon Pinpoint,,,, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3), et. AWS Security Token Service	19 octobre 2022

Modification	Description	Date
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Modification	Description	Date
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Modification	Description	Date
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modification	Description	Date
AWS_ConfigRole – Ajout de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Certificate Manager Amazon Managed Workflows pour Apache Airflow AWS Amplify AWS AppConfig, Amazon Keyspaces, Amazon, Amazon Connect, CloudWatch Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx EventBridge, AWS Fault Injection Service Amazon, Amazon GameLift Location Service, Amazon AWS IoT Lex, Amazon Lightsail, Amazon Pinpoint,,,, Amazon, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition, Amazon Route 53 AWS Resource Groups, Amazon Simple Storage Service AWS Cloud Map(Amazon S3), et. AWS Security Token Service	19 octobre 2022

Modification	Description	Date
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Modification	Description	Date
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Modification	Description	Date
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de Glue::GetTable	Cette politique accorde désormais l'autorisation de récupérer la définition de AWS Glue table dans un catalogue de données pour une table spécifiée.	14 septembre 2022
AWS_ConfigRole – Ajout de Glue::GetTable	Cette politique accorde désormais l'autorisation de récupérer la définition de AWS Glue table dans un catalogue de données pour une table spécifiée.	14 septembre 2022

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR EventBridge, Amazon, Amazon Schemas, Amazon GameLift Fraud Detector Detector, EventBridge Amazon Amazon FinSpace, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service pour Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon, Amazon Route 53 Resolver contrôleur	7 septembre 2022

Modification	Description	Date
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	de restauration d'applications QuickSight Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation, AWS License Manager AWS Resilience Hub, AWS Signer, et AWS Transfer Family.	

Modification	Description	Date
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Modification	Description	Date
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Modification	Description	Date
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Modification	Description	Date
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Modification	Description	Date
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Modification	Description	Date
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Modification	Description	Date
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Modification	Description	Date
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Modification	Description	Date
AWS_ConfigRole – Ajout de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon AppFlow, Amazon CloudWatch, Amazon CloudWatch RUM, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR EventBridge, Amazon, Amazon Schemas, Amazon GameLift Fraud Detector Detector, EventBridge Amazon Amazon FinSpace, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service pour Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon, Amazon Route 53 Resolver contrôleur	7 septembre 2022

Modification	Description	Date
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	de restauration d'applications QuickSight Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation, AWS License Manager AWS Resilience Hub, AWS Signer, et AWS Transfer Family	

Modification	Description	Date
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Modification	Description	Date
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

Modification	Description	Date
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

Modification	Description	Date
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

Modification	Description	Date
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

Modification	Description	Date
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

Modification	Description	Date
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

Modification	Description	Date
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy – Ajout de datasync:ListAgent s, datasync:ListLocations, datasync:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Cette politique autorise désormais à renvoyer une liste d' AWS DataSync agents, d'emplacements DataSync source et de destination et de DataSync tâches dans un Compte AWS ; à répertori er des informations récapitul atives sur les AWS Cloud Map espaces de noms et les services associés à un ou plusieurs espaces de noms spécifiés dans un Compte AWS ; et à répertori er toutes les listes de contacts Amazon Simple Email Service (Amazon SES) disponibles dans. Compte AWS	22 août 2022

Modification	Description	Date
AWS_ConfigRole – Ajout de datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	Cette politique autorise désormais à renvoyer une liste d' AWS DataSync agents, d'emplacements DataSync source et de destination et de DataSync tâches dans un Compte AWS ; à répertorier des informations récapitulatives sur les AWS Cloud Map espaces de noms et les services associés à un ou plusieurs espaces de noms spécifiés dans un Compte AWS ; et à répertorier toutes les listes de contacts Amazon Simple Email Service (Amazon SES) disponibles dans. Compte AWS	22 août 2022
ConfigConformsServiceRolePolicy – Ajout de cloudwatch:PutMetricData	Cette politique autorise désormais la publication de points de données métriques sur Amazon CloudWatch.	25 juillet 2022

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync: DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon ElastiCache, Amazon FSx EventBridge, Amazon Managed Service pour Apache Flink, Amazon Location Service, Amazon Managed Streaming pour Apache Kafka, Amazon, Amazon Rekognition, QuickSight Amazon Simple Storage Service (Amazon S3) Service AWS Billing Conductor S3/, Amazon Simple Email Service (Amazon SES),,,,,,, (IAM Identity Center) AWS Amplify AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center , EC2 Image Builder et Elastic Load Balancing. AWS RoboMaker AWS AppConfig AWS AppSync	15 juillet 2022

Modification	Description	Date
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

Modification	Description	Date
ions, imagebuilder: ListCompo nents, imagebuilder:GetDist ributionConfiguration, imag ebuilder:GetInfrastructureC onfiguration, imagebuilder: ListDistributionConfigurati ons, imagebuilder:ListInfra structureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kines isanalytics:DescribeApplica tion, kinesisanalytics:List TagsForResource, quicksight :DescribeDataSource, quicksight:DescribeDataS ourcePermissions, quicksigh t:ListTagsForResource, reko gnition:DescribeStreamProce ssor, rekognition:ListTagsF orResource, robomaker:Descr ibeRobotApplication, roboma ker:DescribeSimulationAppli cation, s3:GetStorageLensCo nfiguration, s3:GetStorageL ensConfigurationTagging, se rvicediscovery:GetInstance, servicediscovery:GetNamespa ce, servicediscovery:GetSer vice, servicediscovery:List TagsForResource, ses:Descr ibeReceiptRule, ses:Describ eReceiptRuleSet, ses:GetCo ntactList, ses:GetEmailTemp late, ses:GetTemplate, and		

Modification	Description	Date
sso:GetInlinePolicyForPermissionSet		

Modification	Description	Date
AWS_ConfigRole – Ajout de amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	Cette politique prend désormais en charge des autorisations supplémentaires pour Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon ElastiCache, Amazon FSx EventBridge, Amazon Managed Service pour Apache Flink, Amazon Location Service, Amazon Managed Streaming pour Apache Kafka, Amazon, Amazon Rekognition, QuickSight Amazon Simple Storage Service (Amazon S3) Service AWS Billing Conductor S3/, Amazon Simple Email Service (Amazon SES),,,,,,, (IAM Identity Center) AWS Amplify AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center , EC2 Image Builder et Elastic Load Balancing. AWS RoboMaker AWS AppConfig AWS AppSync	15 juillet 2022

Modification	Description	Date
scribeLocationS3, datasync: DescribeLocationSmb, datasy nc:DescribeTask, datasync: ListTagsForResource, ecr:De scribePullThroughCacheRules , ecr:DescribeRegistry, ecr:G etRegistryPolicy, elasticac he:DescribeCacheParameters, elasticloadbalancing:Descr ibeListenerCertificates, el asticloadbalancing:Describe TargetGroupAttributes, elas ticloadbalancing:DescribeTa rgetGroups, elasticloadbala ncing:DescribeTargetHealth, events:DescribeApiDestinat ion, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListP olicies, fms:ListTagsForRes ource, fsx:DescribeVolumes, geo:DescribeGeofenceColl ection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator , geo:DescribeTracker, geo:ListTrackerConsumers, g lue:BatchGetJobs, glue:Batc hGetWorkflows, glue:GetC rawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuil der: GetComponent, imagebuil der: ListComponentBuildVers ions, imagebuilder: ListCompo		

Modification	Description	Date
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Modification	Description	Date
sso:GetInlinePolicyForPermissionSet		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAtt	Cette politique autorise désormais à obtenir un catalogue de données Amazon Athena spécifié, à répertorier les catalogues de données Athena dans un et à répertorier les balises associées à un Compte AWS groupe de travail ou à une ressource de catalogue de données Athena ; à obtenir une liste de graphes de comportement Amazon Detective et à répertorier les balises d'un graphe de comportement de détective ; à obtenir une liste de métadonnées de ressources pour une liste donnée de noms de points de terminaison de développement, à obtenir des informations sur un point de AWS Glue développement spécifique, à obtenir tous les AWS Glue développements points de terminaison dans un, récupèrent une sécurité spécifiée AWS Glue Compte AWS AWS Glue configuration, obtenir toutes les configurations de AWS Glue sécurité, obtenir une liste des balises associées à une AWS Glue ressource, obtenir	31 mai 2022

Modification	Description	Date
ributeConfiguration, sso:DescribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	des informations sur un AWS Glue groupe de travail portant le nom spécifié, récupérer les noms de toutes les ressources d'un AWS compte, obtenir les noms de toutes les ressources d'un, AWS Glue répertorier les noms de toutes les AWS Glue `DevEndpoint` ressources AWS Glue professionnelles d'un compte Compte AWS, obtenir des détails sur les comptes des AWS Glue membres Compte AWS, répertorier les noms des AWS Glue flux de travail créés dans un compte et répertorier les AWS Glue groupes de travail disponibles pour un compte ; pour récupérer des informations sur un GuardDuty filtre Amazon, récupérer un GuardDuty IPSet, récupérer un GuardDuty ThreatIntel ensemble, récupérer des comptes GuardDuty membres, obtenir une liste de GuardDuty filtres, obtenir les IPsets du GuardDuty service, récupérer des balises pour le service et obtenir le nom ThreatIntelSets du GuardDuty GuardDuty service ; pour obtenir le statut actuel et les paramètres de configuration d'un	

Modification	Description	Date
	compte Amazon Macie ; pour récupérer la ressource et les principales associations AWS Resource Access Manager pour AWS RAM() les partages de ressources et obtenir des informations AWS RAM sur les partages de ressources ; pour obtenir des informations sur un ensemble de configuration existant d'Amazon Simple Email Service (Amazon SES), obtenir une liste des destinations d'événements associées à un ensemble de configuration Amazon SES et répertorier tous les ensembles de configuration associés à un compte Amazon SES ; et pour obtenir une liste des attributs de répertoire Identity Center, obtenir les détails d' AWS IAM Identity Center un ensemble d'autorisations, obtenir la politique gérée IAM associée à un ensemble d'autorisations IAM Identity Center spécifié, obtenez les autorisations définies pour une instance IAM Identity Center et obtenez des balises pour IAM Identity Center ressources.	

Modification	Description	Date
AWS_ConfigRole – Ajout de athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	Cette politique autorise désormais à obtenir un catalogue de données Amazon Athena spécifié, à répertorier les catalogues de données Athena dans un et à répertorier les balises associées à un Compte AWS groupe de travail ou à une ressource de catalogue de données Athena ; à obtenir une liste de graphes de comportement Amazon Detective et à répertorier les balises d'un graphe de comportement de détective ; à obtenir une liste de métadonnées de ressources pour une liste donnée de noms de points de terminaison de développement, à obtenir des informations sur un point de AWS Glue développement spécifique, à obtenir tous les AWS Glue développements points de terminaison dans un, récupèrent une sécurité spécifiée AWS Glue Compte AWS AWS Glue configuration, obtenir toutes les configurations de AWS Glue sécurité, obtenir une liste des balises associées à une AWS Glue ressource, obtenir	31 mai 2022

Modification	Description	Date
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	des informations sur un AWS Glue groupe de travail portant le nom spécifié, récupérer les noms de toutes les ressources d'un AWS compte, obtenir les noms de toutes les ressources d'un, AWS Glue répertorier les noms de toutes les AWS Glue `DevEndpoint` ressources AWS Glue professionnelles d'un compte Compte AWS, obtenir des détails sur les comptes des AWS Glue membres Compte AWS, répertorier les noms des AWS Glue flux de travail créés dans un compte et répertorier les AWS Glue groupes de travail disponibles pour un compte ; pour récupérer des informations sur un GuardDuty filtre Amazon, récupérer un GuardDuty IPSet, récupérer un GuardDuty ThreatIntel ensemble, récupérer des comptes GuardDuty membres, obtenir une liste de GuardDuty filtres, obtenir les IPsets du GuardDuty service, récupérer des balises pour le service et obtenir le nom ThreatIntelSets du GuardDuty GuardDuty service ; pour obtenir le statut actuel et les paramètres de configuration d'un	

Modification	Description	Date
	compte Amazon Macie ; pour récupérer la ressource et les principales associations AWS Resource Access Manager pour AWS RAM() les partages de ressources et obtenir des informations AWS RAM sur les partages de ressources ; pour obtenir des informations sur un ensemble de configuration existant d'Amazon Simple Email Service (Amazon SES), obtenir une liste des destinations d'événements associées à un ensemble de configuration Amazon SES et répertorier tous les ensembles de configuration associés à un compte Amazon SES ; et pour obtenir une liste des attributs de répertoire Identity Center, obtenir les détails d' AWS IAM Identity Center un ensemble d'autorisations, obtenir la politique gérée IAM associée à un ensemble d'autorisations IAM Identity Center spécifié, obtenez les autorisations définies pour une instance IAM Identity Center et obtenez des balises pour IAM Identity Center ressources.	

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Cette politique permet désormais d'obtenir des informations sur tout ou un magasin de données d' AWS CloudTrail événements (EDS) spécifique, d'obtenir des informations sur toutes les ressources ou sur une AWS CloudFormation ressource spécifiée, d'obtenir la liste d'un groupe de paramètres ou d'un groupe de sous-réseaux de l'accélérateur DynamoDB (DAX), d'obtenir des informations AWS Database Migration Service sur AWS DMS() les tâches de réplication pour votre compte dans la région actuellement consultée et d'obtenir une liste de toutes les politiques d'un type spécifié. AWS Organizations	7 avril 2022

Modification	Description	Date
AWS_ConfigRole – Ajout de cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Cette politique permet désormais d'obtenir des informations sur tout ou un magasin de données d' AWS CloudTrail événements (EDS) spécifique, d'obtenir des informations sur toutes les ressources ou sur une AWS CloudFormation ressource spécifiée, d'obtenir la liste d'un groupe de paramètres ou d'un groupe de sous-réseaux de l'accélérateur DynamoDB (DAX), d'obtenir des informations AWS Database Migration Service sur AWS DMS() les tâches de réplication pour votre compte dans la région actuellement consultée et d'obtenir une liste de toutes les politiques d'un type spécifié. AWS Organizations	7 avril 2022

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Backup AWS Batch, DynamoDB Accelerator, AWS Database Migration Service Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon,,, Amazon Relational Database Service, V2 et Amazon. GuardDuty AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	14 mars 2022

Modification	Description	Date
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Modification	Description	Date
AWS_ConfigRole – Ajout de backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	Cette politique prend désormais en charge des autorisations supplémentaires pour AWS Backup AWS Batch, DynamoDB Accelerator, AWS Database Migration Service Amazon DynamoDB, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx, Amazon,,, Amazon Relational Database Service, V2 et Amazon. GuardDuty AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	14 mars 2022

Modification	Description	Date
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Cette politique autorise désormais à obtenir des informations sur les environnements Elastic Beanstalk et une description des paramètres du jeu de configuration Elastic Beanstalk spécifié, à obtenir une carte des versions d'Elasticsearch, à décrire les groupes d'options Amazon RDS disponibles pour une base OpenSearch de données et à obtenir des informations sur une configuration de déploiement. CodeDeploy Cette politique autorise également désormais à récupérer le contact alternatif spécifié attaché à une Compte AWS, à récupérer des informations sur une politique, à récupérer une AWS Organizations politique de référentiel Amazon ECR, à récupérer des informations sur une AWS Config règle archivée, à récupérer une liste des familles de définitions de tâches Amazon ECS, à répertorier les unités organisationnelles (UO) racine ou parent de l'unité d'organisation ou du compte enfant spécifié, et à répertorier les politique	10 février 2022

Modification	Description	Date
	s associées à la racine, à l'unité organisationnelle ou au compte cible spécifié.	

Modification	Description	Date
AWS_ConfigRole – Ajout de elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Cette politique autorise désormais à obtenir des informations sur les environnements Elastic Beanstalk et une description des paramètres du jeu de configuration Elastic Beanstalk spécifié, à obtenir une carte des versions d'Elasticsearch, à décrire les groupes d'options Amazon RDS disponibles pour une base OpenSearch de données et à obtenir des informations sur une configuration de déploiement. CodeDeploy Cette politique autorise également désormais à récupérer le contact alternatif spécifié attaché à une Compte AWS, à récupérer des informations sur une politique, à récupérer une AWS Organizations politique de référentiel Amazon ECR, à récupérer des informations sur une AWS Config règle archivée, à récupérer une liste des familles de définitions de tâches Amazon ECS, à répertorier les unités organisationnelles (UO) racine ou parent de l'unité d'organisation ou du compte enfant spécifié, et à répertorier les politique	10 février 2022

Modification	Description	Date
	s associées à la racine, à l'unité organisationnelle ou au compte cible spécifié.	
AWSConfigServiceRolePolicy – Ajout de logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Cette politique accorde désormais l'autorisation de créer des groupes de CloudWatch journaux et des flux Amazon et d'écrire des journaux dans les flux de journaux créés.	15 décembre 2021
AWS_ConfigRole – Ajout de logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Cette politique accorde désormais l'autorisation de créer des groupes de CloudWatch journaux et des flux Amazon et d'écrire des journaux dans les flux de journaux créés.	15 décembre 2021

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Cette politique autorise désormais à obtenir des informations sur un ou plusieurs domaines Amazon OpenSearch Service (OpenSearch Service) et à obtenir une liste de paramètres détaillée pour un groupe de paramètres de base de données Amazon Relational Database Service (Amazon RDS) particulier. Cette politique accorde également l'autorisation d'obtenir des informations sur les ElastiCache instantanés Amazon.	8 septembre 2021
AWS_ConfigRole – Ajout de es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Cette politique autorise désormais à obtenir des informations sur un ou plusieurs domaines Amazon OpenSearch Service (OpenSearch Service) et à obtenir une liste de paramètres détaillée pour un groupe de paramètres de base de données Amazon Relational Database Service (Amazon RDS) particulier. Cette politique accorde également l'autorisation d'obtenir des informations sur les ElastiCache instantanés Amazon.	8 septembre 2021

Modification	Description	Date
AWSConfigServiceRolePolicy— Ajout logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine et autorisations supplémentaires pour les types de AWS ressources	Cette politique accorde désormais des autorisations pour répertorier les balises d'un groupe de journaux, répertorier les balises d'une machine d'état et répertorier toutes les machines d'état. Cette politique accorde désormais des autorisations pour obtenir des détails sur une machine d'état. Cette politique prend également désormais en charge des autorisations supplémentaires pour Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming pour Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Simple Notification Service,, SageMaker et. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28 juillet 2021

Modification	Description	Date
AWS_ConfigRole— Ajoutez l et ogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine des autorisations supplémen taires pour les types de AWS ressources	Cette politique accorde désormais des autorisations pour répertorier les balises d'un groupe de journaux, répertorier les balises d'une machine d'état et répertorier toutes les machines d'état. Cette politique accorde désormais des autorisations pour obtenir des détails sur une machine d'état. Cette politique prend également désormais en charge des autorisations supplémentaires pour Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming pour Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Simple Notification Service,, SageMaker et. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28 juillet 2021

Modification	Description	Date
AWSConfigServiceRolePolicy— Ajout ssm:DescribeDocumentPermission d'autorisations supplémentaires pour les types de AWS ressources	Cette politique accorde désormais des autorisations pour afficher les autorisations relatives aux documents AWS Systems Manager et aux informations concernant l'analyseur d'accès IAM. Cette politique prend désormais en charge AWS des types de ressources supplémentaires pour Amazon Kinesis, Amazon, ElastiCache Amazon EMR, AWS Network Firewall Amazon Route 53 et Amazon Relational Database Service (Amazon RDS). Ces modifications d'autorisation permettent AWS Config d'invoquer les API en lecture seule requises pour prendre en charge ces types de ressources. Cette politique prend également désormais en charge le filtrage des fonctions Lambda @Edge pour la règle gérée AWS Config lambda-inside-vpc.	8 juin 2021

Modification	Description	Date
AWS_ConfigRole— Ajout ssm:DescribeDocumentPermission d'autorisations supplémentaires pour les types de AWS ressources	Cette politique accorde désormais des autorisations pour afficher les autorisations relatives aux documents AWS Systems Manager et aux informations concernant l'analyseur d'accès IAM. Cette politique prend désormais en charge AWS des types de ressources supplémentaires pour Amazon Kinesis, Amazon, ElastiCache Amazon EMR, AWS Network Firewall Amazon Route 53 et Amazon Relational Database Service (Amazon RDS). Ces modifications d'autorisation permettent AWS Config d'invoquer les API en lecture seule requises pour prendre en charge ces types de ressources. Cette politique prend également désormais en charge le filtrage des fonctions Lambda @Edge pour la règle gérée AWS Config lambda-inside-vpc.	8 juin 2021

Modification	Description	Date
AWSConfigServiceRolePolicy – Ajout de l'autorisation apigateway:GET pour effectuer des appels GET en lecture seule vers l'API Gateway et des autorisations s3:GetAccessPointPolicy et s3:GetAccessPointPolicyStatus pour invoquer les API Amazon S3 en lecture seule	Cette politique accorde désormais des autorisations qui permettent d' AWS Config effectuer des appels GET en lecture seule à API Gateway afin de prendre en charge une AWS Config règle pour API Gateway. La politique ajoute également des autorisations qui permettent AWS Config d'invoquer les API en lecture seule d'Amazon Simple Storage Service (Amazon S3), qui sont nécessaires pour prendre en charge le nouveau type de ressource. `AWS::S3::AccessPoint`	10 mai 2021

Modification	Description	Date
AWS_ ConfigRole — Ajoutez apigateway:GET l'autorisation d'effectuer des appels GET en lecture seule à API Gateway et l's3:GetAccessPointPolicyautorisation et s3:GetAccessPointPolicyStatus l'autorisation d'invoquer les API en lecture seule d'Amazon S3	Cette politique accorde désormais des autorisations qui permettent d' AWS Config effectuer des appels GET en lecture seule à API Gateway afin de prendre en charge une passerelle AWS Config pour API. La politique ajoute également des autorisations qui permettent AWS Config d'invoquer les API en lecture seule d'Amazon Simple Storage Service (Amazon S3), qui sont nécessaires pour prendre en charge le nouveau type de ressource. `AWS::S3::AccessPoint`	10 mai 2021

Modification	Description	Date
AWSConfigServiceRolePolicy— Ajoutez des ssm:ListDocuments autorisations et des autorisations supplémentaires pour les types de AWS ressources	Cette politique accorde désormais des autorisations pour afficher des informations sur des documents AWS Systems Manager spécifiés. Cette politique prend également désormais en charge AWS des types de ressources supplémentaires pour AWS Backup Amazon Elastic File System ElastiCache, Amazon, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis SageMaker, Amazon et Amazon Route 53 AWS Database Migration Service. Ces modifications d'autorisation permettent AWS Config d'invoquer les API en lecture seule requises pour prendre en charge ces types de ressources.	1 avril 2021

Modification	Description	Date
AWS_ConfigRole— Ajoutez des ssm:ListDocuments autorisations et des autorisat ions supplémentaires pour les types de AWS ressources	Cette politique accorde désormais des autorisations pour afficher des informati ons sur des documents AWS Systems Manager spécifiés. Cette politique prend également désormais en charge AWS des types de ressources supplémentaires pour AWS Backup Amazon Elastic File System ElastiCac he, Amazon, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis SageMaker, Amazon et Amazon Route 53 AWS Database Migration Service. Ces modifications d'autoris ation permettent AWS Config d'invoquer les API en lecture seule requises pour prendre en charge ces types de ressources.	1 avril 2021
`AWSConfigRole` est obsolète	`AWSConfigRole` est obsolète `AWS_ConfigRole` est la politique de remplacem ent.	1 avril 2021
AWS Config a commencé à suivre les modifications	AWS Config a commencé à suivre les modifications apportées AWS à ses politique s gérées.	1 avril 2021

Autorisations pour le rôle IAM attribué à AWS Config

Un rôle IAM vous permet de définir un ensemble d'autorisations. AWS Config assume le rôle que vous lui attribuez pour écrire dans votre compartiment S3, publier sur votre rubrique SNS et envoyer des demandes `Describe` d'`List`API pour obtenir les détails de configuration de vos AWS ressources. Pour plus d'informations sur les rôles IAM, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

Lorsque vous utilisez la AWS Config console pour créer ou mettre à jour un rôle IAM, les autorisations requises vous sont AWS Config automatiquement associées. Pour plus d'informations, consultez Configuration à l' AWS Config aide de la console.

Table des matières

- Création de politiques de rôle IAM
  - Ajout d'une politique d'approbation IAM à votre rôle
  - Politique de rôle IAM pour le compartiment S3
  - Politique de rôle IAM pour la clé KMS
  - Politique de rôle IAM pour la rubrique Amazon SNS
  - Politique de rôle IAM pour obtenir des détails de configuration
- Gestion des autorisations pour l'enregistrement du compartiment S3

Création de politiques de rôle IAM

Lorsque vous utilisez la AWS Config console pour créer un rôle IAM, les autorisations requises sont AWS Config automatiquement associées au rôle pour vous.

Si vous utilisez le AWS CLI pour configurer AWS Config ou si vous mettez à jour un rôle IAM existant, vous devez mettre à jour manuellement la politique pour autoriser l'accès AWS Config à votre compartiment S3, publier sur votre rubrique SNS et obtenir les détails de configuration de vos ressources.

Ajout d'une politique d'approbation IAM à votre rôle

Vous pouvez créer une politique de confiance IAM qui permet d' AWS Config assumer un rôle et de l'utiliser pour suivre vos ressources. Pour plus d'informations sur les politiques d'approbation IAM, consultez Termes et concepts relatifs aux rôles dans le Guide de l'utilisateur IAM.

Voici un exemple de politique de confiance pour les AWS Config rôles :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Vous pouvez utiliser la condition `AWS:SourceAccount` de la relation d'approbation du rôle IAM susmentionnée pour limiter le principal du service Config, en lui permettant uniquement d'interagir avec le rôle AWS IAM lorsqu'il effectue des opérations au nom de comptes spécifiques.

AWS Config prend également en charge la `AWS:SourceArn` condition qui empêche le principal du service Config d'assumer le rôle IAM uniquement lorsqu'il effectue des opérations pour le compte propriétaire. Lorsque vous utilisez le principal de AWS Config service, la `AWS:SourceArn` propriété sera toujours définie sur la région de l'enregistreur de configuration et `sourceAccountID` sur l'ID du compte contenant l'enregistreur de configuration. `arn:aws:config:sourceRegion:sourceAccountID:* sourceRegion` Pour plus d'informations sur l'enregistreur AWS Config de configuration, voir Gestion de l'enregistreur de configuration. Ajoutez par exemple la condition suivante pour restreindre le principal du service Config afin qu'il assume le rôle IAM uniquement pour le compte d'un enregistreur de configuration de la région `us-east-1` dans le compte `123456789012` :`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Politique de rôle IAM pour le compartiment S3

L'exemple de politique suivant accorde AWS Config l'autorisation d'accéder à votre compartiment S3 :

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::myBucketName"
    }
  ]
}
```

Politique de rôle IAM pour la clé KMS

L'exemple de politique suivant AWS Config autorise l'utilisation du chiffrement basé sur KMS sur de nouveaux objets pour la livraison du compartiment S3 :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
```

```
        }
    ]
}
```

Politique de rôle IAM pour la rubrique Amazon SNS

L'exemple de politique suivant accorde AWS Config l'autorisation d'accéder à votre rubrique SNS :

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

Si votre rubrique SNS est chiffrée, consultez Configuration des autorisations AWS KMS dans le Guide du développeur Amazon Simple Notification Service pour obtenir des instructions de configuration supplémentaires.

Politique de rôle IAM pour obtenir des détails de configuration

Pour enregistrer vos configurations de AWS ressources, vous AWS Config devez disposer des autorisations IAM pour obtenir les détails de configuration de vos ressources.

Utilisez la politique AWS gérée AWS_ ConfigRole et attachez-la au rôle IAM que vous attribuez. AWS Config AWS met à jour cette politique chaque fois qu'elle AWS Config ajoute la prise en charge d'un type de AWS ressource, ce qui signifie que nous AWS Config continuerons à disposer des autorisations requises pour obtenir les détails de configuration tant que cette politique gérée est attachée au rôle.

Si vous créez ou mettez à jour un rôle avec la console, associez AWS Config l'AWS_ ConfigRole pour vous.

Si vous utilisez le AWS CLI, utilisez la `attach-role-policy` commande et spécifiez le nom de ressource Amazon (ARN) pour AWS_ ConfigRole :

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
```

Gestion des autorisations pour l'enregistrement du compartiment S3

AWS Config enregistre et envoie des notifications lorsqu'un compartiment S3 est créé, mis à jour ou supprimé.

Il est recommandé d'utiliser `AWSServiceRoleForConfig` (voir Utilisation des rôles liés à un service pour AWS Config) ou un rôle IAM personnalisé utilisant la politique `AWS_ConfigRole` gérée. Pour plus d'informations sur les bonnes pratiques en matière d'enregistrement de configuration, consultez Bonnes pratiques AWS Config.

Si vous devez gérer les autorisations au niveau de l'objet pour l'enregistrement de votre compartiment, assurez-vous, dans la politique du compartiment S3, de fournir `config.amazonaws.com` (le nom principal du AWS Config service) un accès à toutes les autorisations associées à S3 issues de la politique `AWS_ConfigRole` gérée. Pour de plus d'informations, consultez Autorisations pour le compartiment Amazon S3.

Mise à jour du rôle IAM attribué à AWS Config

Vous pouvez mettre à jour le rôle IAM assumé à AWS Config tout moment. Avant de mettre à jour le rôle IAM vérifiez que vous avez créé un nouveau rôle pour remplacer l'ancien. Vous devez associer au nouveau rôle des politiques autorisant l'enregistrement des AWS Config configurations et leur transmission à votre canal de diffusion. En outre, prenez soin de copier l'Amazon Resource Name (ARN) de votre nouveau rôle IAM. Vous en aurez besoin pour mettre à jour le rôle IAM. Pour en savoir plus sur la création d'un rôle IAM et l'association des politiques requises pour le rôle IAM, consultez Création d'un rôle IAM.

> **Note**
>
> Pour trouver l'ARN d'un rôle IAM existant, accédez à la console IAM à l'adresse https://console.aws.amazon.com/iam/. Choisissez Rôles dans le panneau de navigation. Choisissez ensuite le nom du rôle souhaité et trouvez l'ARN en haut de la page Récapitulatif.

Mise à jour du rôle IAM

Vous pouvez mettre à jour votre rôle IAM à l'aide du AWS Management Console ou du AWS CLI.

To update the IAM role (Console)

Si vous l'utilisez AWS Config dans une région où les AWS Config règles sont prises en charge, procédez comme suit. Pour obtenir la liste des régions prises en charge, consultez la section Régions et points de terminaison AWS Config dans le Référence générale d'Amazon Web Services.

1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config/.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Choisissez Modifier sur la page Paramètres.
4. Dans la section Gouvernance des données, choisissez le rôle IAM pour AWS Config :
   - Utiliser un rôle AWS Config lié à un service existant : AWS Config crée un rôle doté des autorisations requises.
   - Choisissez un rôle dans votre compte : pour les rôles existants, choisissez un rôle IAM dans votre compte.
5. Choisissez Enregistrer.

To update the IAM role (AWS CLI)

Utilisez la commande `put-configuration-recorder` et spécifiez l'Amazon Resource Name (ARN) du nouveau rôle :

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

Autorisations pour le compartiment Amazon S3 pour le canal AWS Config de diffusion

> **Important**
>
> Cette page explique comment configurer le compartiment Amazon S3 pour le canal AWS Config de diffusion. Cette page ne traite pas du type de `AWS::S3::Bucket` ressource que

l'enregistreur AWS Config de configuration peut enregistrer. Pour plus d'informations sur le canal AWS Config de diffusion, consultez la section Gestion du canal de diffusion.

Par défaut, tous les objets et les compartiments Amazon S3 sont privés. Seul le propriétaire de la ressource Compte AWS qui a créé le compartiment peut accéder à ce compartiment. Le propriétaire de la ressource peut toutefois accorder des autorisations d'accès à d'autres ressources et à d'autres utilisateurs. Une solution consiste à écrire une stratégie d'accès.

Si un compartiment Amazon S3 est AWS Config créé automatiquement pour vous (par exemple, si vous utilisez AWS Config la console pour configurer votre canal de diffusion), ces autorisations sont automatiquement ajoutées au compartiment Amazon S3. Toutefois, si vous spécifiez un compartiment Amazon S3 existant, vous devez vous assurer que le compartiment S3 dispose des autorisations appropriées.

> **Note**
>
> un objet n'hérite pas des autorisations de son compartiment. Par exemple, si vous créez un compartiment et accordez un accès en écriture à un utilisateur, vous ne pouvez pas accéder à ses objets sauf s'il vous accorde explicitement l'accès.

Table des matières

- Autorisations requises pour le compartiment Amazon S3 lors de l'utilisation de rôles IAM
- Autorisations requises pour le compartiment Amazon S3 lors de l'utilisation de rôles liés à un service
- Octroi de l' AWS Config accès au compartiment Amazon S3

Autorisations requises pour le compartiment Amazon S3 lors de l'utilisation de rôles IAM

Lorsque AWS Config vous envoyez des informations de configuration (fichiers d'historique et instantanés) au compartiment Amazon S3 de votre compte, il assume le rôle IAM que vous avez attribué lors de la configuration. AWS Config Lorsqu' AWS Config envoie les informations de configuration à un compartiment Amazon S3 d'un autre compte, il tente d'abord d'utiliser le rôle IAM, mais cette tentative échoue si la stratégie d'accès pour le compartiment n'accorde pas l'accès `WRITE` au rôle IAM. Dans ce cas, AWS Config envoie à nouveau les informations, cette fois en

tant que principal du AWS Config service. Pour que la livraison puisse réussir, la politique d'accès doit autoriser l'`WRITE`accès au nom `config.amazonaws.com` principal. AWS Config est alors le propriétaire des objets qu'il livre au compartiment S3. Vous devez attacher une stratégie d'accès (mentionnée à l'étape 6 ci-dessous) au compartiment Amazon S3 d'un autre compte pour accorder à AWS Config un accès à ce compartiment Amazon S3.

Avant de AWS Config pouvoir envoyer des journaux à votre compartiment Amazon S3, AWS Config vérifie si le compartiment existe et dans quelle AWS région il se trouve. AWS Config tente d'appeler HeadBucketl'API Amazon S3 pour vérifier si le compartiment existe et pour obtenir la région du compartiment. Si aucune autorisation n'est fournie pour localiser le compartiment lors de la vérification de localisation, une `AccessDenied` erreur s'affiche dans AWS CloudTrail les journaux. Toutefois, la diffusion des journaux est effectuée dans votre compartiment Amazon S3 si vous ne fournissez pas d'autorisations sur l'emplacement de ce dernier.

> **Note**
>
> Pour accorder une autorisation à l'API Amazon S3 `HeadBucket`, autorisez l'exécution de l'action `s3:ListBucket` en tant que Sid `AWSConfigBucketExistenceCheck`, comme indiqué à l'étape 6 ci-dessous.

Autorisations requises pour le compartiment Amazon S3 lors de l'utilisation de rôles liés à un service

Le rôle AWS Config lié à un service n'est pas autorisé à placer des objets dans des compartiments Amazon S3. Ainsi, si vous configurez AWS Config en utilisant un rôle lié à un service, il AWS Config enverra plutôt les éléments de configuration en tant que principal du AWS Config service. Vous devrez joindre une politique d'accès, mentionnée à l'étape 6 ci-dessous, au compartiment Amazon S3 dans votre propre compte ou sur un autre compte pour autoriser l' AWS Config accès au compartiment Amazon S3.

Octroi de l' AWS Config accès au compartiment Amazon S3

Suivez les étapes ci-dessous pour ajouter une stratégie d'accès au compartiment Amazon S3 dans votre propre compte ou dans un autre compte. La politique d'accès permet AWS Config d'envoyer des informations de configuration à un compartiment Amazon S3.

1. Connectez-vous à l' AWS Management Console aide du compte qui possède le compartiment S3.

2. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
3. Sélectionnez le compartiment que vous souhaitez utiliser AWS Config pour fournir les éléments de configuration, puis choisissez Propriétés.
4. Choisissez Autorisations.
5. Choisissez Modifier la stratégie de compartiment.
6. Copiez la stratégie suivante dans la fenêtre Éditeur de stratégie de compartiment :

> **Important**
>
> Pour des raisons de sécurité, lorsque vous autorisez AWS Config l'accès à un compartiment Amazon S3, nous vous recommandons vivement de restreindre l'accès dans le cadre de la politique de compartiment à `AWS:SourceAccount` cette condition. Si votre politique de compartiment existante ne suit pas cette bonne pratique de sécurité, nous vous recommandons vivement de la modifier pour inclure cette protection. Cela garantit que l'accès AWS Config est accordé au nom des utilisateurs attendus uniquement.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

> **Note**
>
> Lorsque vous accordez des autorisations à votre rôle IAM au lieu du nom principal du AWS Config service (SPN), assurez-vous que votre rôle IAM dispose d'une `PutObjectACL` autorisation sur le bucket multi-comptes afin d'éviter toute erreur d'autorisation insuffisante. Consultez un exemple de politique de rôle IAM à l'adresse Politique de rôle IAM pour le compartiment S3.

7. Remplacez les valeurs suivantes dans la stratégie de compartiment :

   - *`target BucketName`* : nom du compartiment Amazon S3 auquel les éléments de configuration AWS Config seront envoyés.

- *[optional] prefix* : ajout facultatif à la clé d'objet Amazon S3 qui permet de créer une organisation de type dossier dans le compartiment.
- *sourceAccountId* — L'ID du compte pour lequel les éléments de configuration AWS Config seront envoyés au compartiment cible.

8. Choisissez Enregistrer, puis Fermer.

Vous pouvez utiliser la condition `AWS:SourceAccount` de la politique de compartiment Amazon S3 susmentionnée pour limiter le principal du service Config, en lui permettant uniquement d'interagir avec le compartiment Amazon S3 lorsqu'il effectue des opérations au nom de comptes spécifiques. Si vous envisagez de configurer AWS Config plusieurs comptes de la même organisation pour fournir des éléments de configuration à un seul compartiment Amazon S3, nous vous recommandons d'utiliser des rôles IAM plutôt que des rôles liés à un service afin de pouvoir utiliser des clés de AWS Organizations conditions telles que. `AWS:PrincipalOrgID` Pour plus d'informations sur la gestion des autorisations d'accès associées à un rôle IAM à utiliser AWS Config, consultez la section Autorisations relatives au rôle IAM attribué à. AWS Config Pour plus d'informations sur la gestion des autorisations d'accès pour AWS Organizations, consultez la section Gestion des autorisations d'accès pour votre AWS organisation.

AWS Config prend également en charge la `AWS:SourceArn` condition qui interdit au principal du service Config d'interagir uniquement avec le compartiment Amazon S3 lorsqu'il effectue des opérations pour le compte de canaux de AWS Config distribution spécifiques. Lorsque vous utilisez le principal de AWS Config service, la `AWS:SourceArn` propriété sera toujours définie comme `sourceRegion` étant la région du canal de livraison et `sourceAccountID` l'identifiant du compte contenant le canal de livraison. `arn:aws:config:sourceRegion:sourceAccountID:*` Pour plus d'informations sur les canaux AWS Config de diffusion, consultez la section Gestion du canal de diffusion. Ajoutez par exemple la condition suivante pour limiter le principal du service Config en lui permettant d'interagir avec votre compartiment Amazon S3 uniquement pour le compte d'un canal de livraison dans la région `us-east-1` du compte `123456789012` :`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Autorisations relatives à la clé KMS pour le canal AWS Config de distribution

Utilisez les informations de cette rubrique si vous souhaitez créer une politique pour une AWS KMS clé pour votre compartiment S3 qui vous permette d'utiliser le chiffrement basé sur le KMS sur les objets fournis par AWS Config pour la livraison du compartiment S3.

Table des matières

- Autorisations requises pour la clé KMS lors de l'utilisation de rôles IAM (diffusion de compartiment S3)
- Autorisations requises pour la AWS KMS clé lors de l'utilisation de rôles liés à un service (livraison du compartiment S3)
- Octroi de l' AWS Config accès à la AWS KMS clé

Autorisations requises pour la clé KMS lors de l'utilisation de rôles IAM (diffusion de compartiment S3)

Si vous configurez à AWS Config l'aide d'un rôle IAM, vous pouvez associer la politique d'autorisation suivante à la clé KMS :

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> Si le rôle IAM, la politique du compartiment Amazon S3 ou la AWS KMS clé ne fournissent pas un accès approprié AWS Config, AWS Config la tentative d'envoi des informations de configuration au compartiment Amazon S3 échouera. Dans ce cas, AWS Config envoie à nouveau les informations, cette fois en tant que principal du AWS Config service. Dans ce cas, vous devez joindre une politique d'autorisation, mentionnée ci-dessous, à la AWS KMS clé pour AWS Config autoriser l'utilisation de la clé lors de la transmission d'informations au compartiment Amazon S3.

Autorisations requises pour la AWS KMS clé lors de l'utilisation de rôles liés à un service (livraison du compartiment S3)

Le rôle AWS Config lié au service n'est pas autorisé à accéder à la AWS KMS clé. Ainsi, si vous configurez AWS Config en utilisant un rôle lié à un service, il AWS Config enverra des informations en tant que principal de AWS Config service à la place. Vous devrez joindre une politique d'accès, mentionnée ci-dessous, à la AWS KMS clé pour autoriser AWS Config l'utilisation de la AWS KMS clé lors de la transmission d'informations au compartiment Amazon S3.

Octroi de l' AWS Config accès à la AWS KMS clé

Cette politique permet d' AWS Config utiliser une AWS KMS clé lors de la transmission d'informations à un compartiment Amazon S3

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
```

```
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Remplacez les valeurs suivantes dans la stratégie de clé :

- *MyKMSKeyarn* — L'ARN de la AWS KMS clé utilisée pour chiffrer les données dans le compartiment Amazon S3 auquel les éléments de configuration AWS Config seront envoyés.
- *sourceAccountID* : l'ID du compte pour lequel AWS Config fournira les éléments de configuration.

Vous pouvez utiliser la `AWS:SourceAccount` condition de la politique de AWS KMS clé ci-dessus pour empêcher le principal du service Config d'interagir uniquement avec la AWS KMS clé lorsqu'il effectue des opérations pour le compte de comptes spécifiques.

AWS Config prend également en charge la `AWS:SourceArn` condition qui interdit au principal du service Config d'interagir uniquement avec le compartiment Amazon S3 lorsqu'il effectue des opérations pour le compte de canaux de AWS Config distribution spécifiques. Lorsque vous utilisez le principal de AWS Config service, la `AWS:SourceArn` propriété sera toujours définie comme `sourceRegion` étant la région du canal de livraison et `sourceAccountID` l'identifiant du compte contenant le canal de livraison. `arn:aws:config:sourceRegion:sourceAccountID:*` Pour plus d'informations sur les canaux AWS Config de diffusion, consultez la section Gestion du canal de diffusion. Ajoutez par exemple la condition suivante pour limiter le principal du service Config en lui permettant d'interagir avec votre compartiment Amazon S3 uniquement pour le compte d'un canal de livraison dans la région `us-east-1` du compte `123456789012` :`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Autorisations relatives à la rubrique Amazon SNS

Cette rubrique décrit comment configurer pour AWS Config diffuser des rubriques Amazon SNS détenues par un autre compte. AWS Config doit disposer des autorisations requises pour envoyer des notifications à une rubrique Amazon SNS. Pour la configuration d'un même compte, lorsque la AWS Config console crée une rubrique Amazon SNS ou que vous choisissez une rubrique Amazon

SNS depuis votre propre compte AWS Config , assurez-vous que la rubrique Amazon SNS inclut les autorisations requises et respecte les meilleures pratiques en matière de sécurité.

> **Note**
>
> AWS Config prend actuellement en charge l'accès uniquement dans la même région et entre les comptes. Les rubriques SNS utilisées pour les documents de correction AWS Systems Manager (SSM) ou pour le canal de distribution de l'enregistreur ne peuvent pas être interrégionales.

Table des matières

- Autorisations requises pour la rubrique Amazon SNS lors de l'utilisation de rôles IAM
- Autorisations requises pour la rubrique Amazon SNS lors de l'utilisation de rôles liés à un service
- Autoriser AWS Config l'accès à la rubrique Amazon SNS.
- Résolution des problèmes liés à la rubrique Amazon SNS

Autorisations requises pour la rubrique Amazon SNS lors de l'utilisation de rôles IAM

Vous pouvez attacher une politique d'autorisation à la rubrique Amazon SNS appartenant à un autre compte. Si vous voulez utiliser une rubrique Amazon SNS d'un autre compte, veillez à attacher la politique suivante à une rubrique Amazon SNS existante.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
```

```
        }
      }
    ]
}
```

Pour la clé `Resource`, *`account-id`* est le numéro de compte AWS du propriétaire de la rubrique. Pour *`account-id1`*, *`account-id2 et account-id3`*, utilisez le qui Comptes AWS enverra des données à une rubrique Amazon SNS. Vous pouvez remplacer *`region`* et *`myTopic`* par les valeurs appropriées.

Lorsque AWS Config vous envoyez une notification à un sujet Amazon SNS, il tente d'abord d'utiliser le rôle IAM, mais cette tentative échoue si le rôle n'est Compte AWS pas autorisé à publier sur le sujet. Dans ce cas, AWS Config envoie à nouveau la notification, cette fois sous la forme d'un nom principal de AWS Config service (SPN). Pour que la publication réussisse, la stratégie d'accès pour la rubrique doit autoriser l'accès `sns:Publish` au nom du principal `config.amazonaws.com`. Vous devez attacher une stratégie d'accès, décrite dans la section suivante, à la rubrique Amazon SNS pour accorder à AWS Config un accès à la rubrique Amazon SNS si le rôle IAM n'est pas autorisé à publier sur la rubrique.

Autorisations requises pour la rubrique Amazon SNS lors de l'utilisation de rôles liés à un service

Le rôle AWS Config lié au service n'est pas autorisé à accéder à la rubrique Amazon SNS. Ainsi, si vous configurez AWS Config en utilisant un rôle lié à un service (SLR), il AWS Config enverra des informations en tant que principal de AWS Config service à la place. Vous devrez joindre une politique d'accès, mentionnée ci-dessous, à la rubrique Amazon SNS pour autoriser l' AWS Config accès à l'envoi d'informations à la rubrique Amazon SNS.

Pour la configuration du même compte, lorsque la rubrique Amazon SNS et le SLR appartiennent au même compte et que la politique Amazon SNS accorde au SLR l'autorisation « `sns:Publish` », vous n'avez pas besoin d'utiliser le SPN AWS Config . La politique d'autorisation ci-dessous et les recommandations relatives aux bonnes pratiques de sécurité concernent la configuration entre comptes.

Autoriser AWS Config l'accès à la rubrique Amazon SNS.

Cette politique permet AWS Config d'envoyer une notification à une rubrique Amazon SNS. Pour autoriser l' AWS Config accès à la rubrique Amazon SNS depuis un autre compte, vous devez joindre la politique d'autorisation suivante.

> **Note**
>
> En tant que bonne pratique en matière de sécurité, il est fortement recommandé de s'assurer que l'accès aux ressources AWS Config est réservé aux utilisateurs attendus en limitant l'accès aux comptes répertoriés dans les `AWS:SourceAccount` conditions requises.

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

Pour la clé `Resource`, *`account-id`* est le numéro de compte AWS du propriétaire de la rubrique. Pour *`account-id1`*, *`account-id2 et account-id3`*, utilisez le qui Comptes AWS enverra des données à une rubrique Amazon SNS. Vous pouvez remplacer *`region`* et *`myTopic`* par les valeurs appropriées.

Vous pouvez utiliser la `AWS:SourceAccount` condition figurant dans la précédente politique relative aux rubriques Amazon SNS pour empêcher le nom principal du AWS Config service (SPN) d'interagir uniquement avec le sujet Amazon SNS lorsque vous effectuez des opérations pour le compte de comptes spécifiques.

AWS Config prend également en charge la `AWS:SourceArn` condition qui restreint le nom principal du AWS Config service (SPN) à interagir uniquement avec le compartiment S3 lors de l'exécution d'opérations pour le compte de canaux de AWS Config distribution spécifiques. Lorsque vous utilisez le nom principal du AWS Config service (SPN), la `AWS:SourceArn` propriété sera toujours définie comme `sourceRegion` étant la région du canal de distribution et `sourceAccountID` l'ID du compte contenant le canal de distribution. `arn:aws:config:sourceRegion:sourceAccountID:*` Pour plus d'informations sur les canaux AWS Config de diffusion, consultez la section Gestion du canal de diffusion. Par exemple, ajoutez la condition suivante pour empêcher le nom principal du AWS Config service (SPN) d'interagir avec votre compartiment S3 uniquement pour le compte d'un canal de diffusion de la `us-east-1` région dans le compte `123456789012` : `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

Résolution des problèmes liés à la rubrique Amazon SNS

AWS Config doit être autorisé à envoyer des notifications à une rubrique Amazon SNS. Si une rubrique Amazon SNS ne peut pas recevoir de notifications, vérifiez que le rôle IAM qu'il AWS Config assumait dispose des autorisations requises. `sns:Publish`

Résolution des problèmes AWS Config d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS Config IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Config
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Config ressources

Je ne suis pas autorisé à effectuer une action dans AWS Config

Si vous recevez une erreur qui indique que vous n’êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d’effectuer l’action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `config:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

Dans ce cas, la stratégie de Mateo doit être mise à jour pour l'autoriser à accéder à la ressource *my-example-widget* à l'aide de l'action `config:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS Config.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS Config. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Config ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques

basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS Config en charge, consultezComment AWS Config fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Utilisation de rôles liés à un service pour AWS Config

AWS Config utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Config Les rôles liés au service sont prédéfinis par AWS Config et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Config car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Config définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Config peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Config

AWS Config utilise le rôle lié au service nommé AWSServiceRoleForConfig: AWS Config utilise ce rôle lié au service pour appeler d'autres AWS services en votre nom.

Le rôle AWSServiceRoleForConfiglié au service fait confiance au `config.amazonaws.com` service pour assumer le rôle.

La politique d'autorisations pour le `AWSServiceRoleForConfig` rôle contient des autorisations en lecture seule et en écriture seule pour les ressources et des autorisations en lecture seule pour les AWS Config ressources des autres services pris en charge. AWS Config Pour consulter la stratégie gérée AWSServiceRoleForConfig, consultez la section stratégies AWS gérées pour AWS Config. Pour plus d'informations, consultez Types de ressource pris en charge.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Pour utiliser un rôle lié à un service avec AWS Config, vous devez configurer les autorisations sur votre compartiment Amazon S3 et sur la rubrique Amazon SNS. Pour plus d'informations, consultez Autorisations requises pour le compartiment Amazon S3 lors de l'utilisation de rôles liés à un service, Autorisations requises pour la AWS KMS clé lors de l'utilisation de rôles liés à un service (livraison du compartiment S3) et Autorisations requises pour la rubrique Amazon SNS lors de l'utilisation de rôles liés à un service.

Création d'un rôle lié à un service pour AWS Config

Dans l'interface de ligne de commande (CLI) IAM ou l'API IAM, créez un rôle lié à un service avec le nom de service `config.amazonaws.com`. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour AWS Config

AWS Config ne vous permet pas de modifier le rôle AWSServiceRoleForConfiglié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Config

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le AWS Config service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Config les ressources utilisées par AWSServiceRoleForConfig

Assurez-vous que `ConfigurationRecorders` n'utilise pas ce rôle lié à un service. Vous pouvez utiliser la AWS Config console pour arrêter l'enregistreur de configuration. Pour arrêter l'enregistrement, sous L'enregistrement est activé, choisissez Désactiver.

Vous pouvez supprimer l' AWS Config API `ConfigurationRecorder` d'utilisation. Pour procéder à la suppression, utilisez la commande `delete-configuration-recorder`.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, la CLI IAM ou l'API IAM pour supprimer le rôle lié au AWSServiceRoleForConfig service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Réponse aux incidents dans AWS Config

La sécurité est la priorité absolue chez AWS. Dans le cadre du modèle de responsabilité partagée du AWS cloud, AWS gère un centre de données, un réseau et une architecture logicielle qui répondent aux exigences des organisations les plus sensibles en matière de sécurité. AWS est responsable

de toute réponse aux incidents concernant le AWS Config service lui-même. De plus, en tant que AWS client, vous partagez la responsabilité du maintien de la sécurité dans le cloud. Cela signifie que vous contrôlez la sécurité que vous choisissez de mettre en œuvre à partir des AWS outils et fonctionnalités auxquels vous avez accès, et que vous êtes responsable de la réponse aux incidents de votre côté dans le cadre du modèle de responsabilité partagée.

En établissant une base de sécurité répondant aux objectifs de vos applications exécutées dans le cloud, vous êtes en mesure de détecter les écarts auxquels vous pouvez réagir. La réponse aux incidents de sécurité étant un sujet complexe, nous vous encourageons à consulter les ressources suivantes afin de mieux comprendre l'impact de la réponse aux incidents (IR) et de vos choix sur les objectifs de votre entreprise : guide de réponse aux incidents de AWS sécurité, livre blanc sur les meilleures pratiques de AWS sécurité et livre blanc sur la perspective de sécurité du cadre d'adoption du AWS cloud (CAF).

Validation de conformité pour AWS Config

Des auditeurs tiers évaluent la sécurité et AWS Config la conformité de plusieurs programmes de AWS conformité. Il s’agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d’autres.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Config

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées,

connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans AWS Config

En tant que service géré, AWS Config il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS Config via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Configuration et analyse des vulnérabilités

Pour AWS Config, AWS gère les tâches de sécurité de base telles que l'application de correctifs au système d'exploitation client (OS) et aux bases de données, la configuration du pare-feu et la reprise après sinistre.

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui AWS Config accordent un autre service à la ressource. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (`*`) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.

L'exemple suivant montre comment vous pouvez utiliser les touches de contexte de condition `aws:SourceAccount` globale `aws:SourceArn` et globale AWS Config pour éviter le problème de confusion lié aux adjoints : accorder l' AWS Config accès au compartiment Amazon S3.

Bonnes pratiques en matière de sécurité pour AWS Config

AWS Config fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être

appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

- Tirez parti du balisage pour AWS Config faciliter la gestion, la recherche et le filtrage des ressources.
- Vérifiez que vos canaux de diffusion ont été correctement configurés et, une fois confirmés, vérifiez que l'enregistrement AWS Config est correct.

Pour plus d'informations, consultez le blog Bonnes pratiques relatives àAWS Config.

Connexion et surveillance AWS Config

AWS Config est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Config. La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS Config et des performances de vos AWS solutions.

Rubriques

- Journalisation des appels d' AWS Config API avec AWS CloudTrail
- Surveillance

Journalisation des appels d' AWS Config API avec AWS CloudTrail

CloudTrail capture tous les appels d'API AWS Config sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Config console et des appels de code vers les opérations de l' AWS Config API. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS Config. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Config, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Rubriques

- AWS Config Informations dans CloudTrail
- Comprendre les entrées du fichier AWS Config journal
- Exemples de fichiers journaux

AWS Config Informations dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AWS Config, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez

consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre région Compte AWS, y compris des événements pour AWS Config, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les AWS Config opérations sont enregistrées CloudTrail et documentées dans la référence de l'AWS Config API. Par exemple, les appels aux opérations DeliverConfigSnapshot, DeleteDeliveryChannel et DescribeDeliveryChannels génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier AWS Config journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Exemples de fichiers journaux

Pour des exemples d'entrées de CloudTrail journal, consultez les rubriques suivantes.

DeleteDeliveryChannel

Voici un exemple de fichier CloudTrail journal pour le fonctionnement du DeleteDeliverycanal.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
```

```
    }
```

DeliverConfigSnapshot

Voici un exemple de fichier CloudTrail journal pour l'opération DeliverConfigSnapshot.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
```

```
    }
```

DescribeConfigurationRecorderStatus

Voici un exemple de fichier CloudTrail journal pour l'DescribeConfigurationRecorderStatusopération.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

Voici un exemple de fichier CloudTrail journal pour l'opération DescribeConfigurationRecorders.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
```

```
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

Voici un exemple de fichier CloudTrail journal pour l'opération DescribeDeliveryChannels.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

Voici un exemple de fichier CloudTrail journal pour l'GetResourceConfigHistoryopération.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
```

```
      }
```

PutConfigurationRecorder

Voici un exemple de fichier CloudTrail journal pour l'opération PutConfigurationRecorder.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

Voici un exemple de fichier CloudTrail journal pour le fonctionnement du PutDeliverycanal.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
```

```
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

Voici un exemple de fichier CloudTrail journal pour l'opération StartConfigurationRecorder.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
```

```
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

Voici un exemple de fichier CloudTrail journal pour l'opération StopConfigurationRecorder.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

Surveillance

Vous pouvez utiliser d'autres AWS services pour surveiller les AWS Config ressources.

- Vous pouvez utiliser Amazon Simple Notification Service (SNS) pour vous envoyer des notifications chaque fois qu'une AWS ressource prise en charge est créée, mise à jour ou modifiée suite à l'activité de l'API utilisateur.
- Vous pouvez utiliser Amazon EventBridge pour détecter les changements de statut des AWS Config événements et y réagir.

Rubriques

- Surveillance des modifications AWS des ressources avec Amazon SQS
- Surveillance AWS Config avec Amazon EventBridge

Surveillance des modifications AWS des ressources avec Amazon SQS

AWS Config utilise Amazon Simple Notification Service (SNS) pour vous envoyer des notifications chaque fois qu'une AWS ressource prise en charge est créée, mise à jour ou modifiée suite à l'activité de l'API utilisateur. Cependant, vous ne vous intéressez peut-être qu'aux changements de configuration de certaines ressources. A titre d'exemple, il pourrait vous sembler essentiel d'être averti de chaque changement de configuration d'un groupe de sécurité, sans pour autant être informé de chaque modification apportée aux balises de vos instances Amazon EC2. Vous pourriez écrire un programme qui exécute des actions spécifiques lorsque des ressources spécifiques sont mises à jour. Par exemple, vous pourriez vouloir démarrer un certain flux de travail lorsque la configuration d'un groupe de sécurité est modifiée. Si vous souhaitez utiliser les données par programmation de AWS Config cette manière ou d'une autre, utilisez une file d'attente Amazon Simple Queue Service comme point de terminaison de notification pour Amazon SNS.

> **Note**
>
> Des notifications peuvent également provenir d'Amazon SNS sous la forme d'un e-mail, de SMS (Short Message Service) envoyés vers des téléphones mobiles qui prennent en charge les SMS et des smartphones, sous la forme d'un message de notification vers une application sur un appareil mobile ou sous la forme d'un message de notification vers un ou plusieurs points de terminaison HTTP ou HTTPS.

Vous pouvez avoir une seule file d'attente SQS pour s'abonner à plusieurs sujets, que vous ayez un sujet pour chaque région ou un sujet pour chaque compte pour chaque région. Vous devez vous abonner à la file d'attente de votre rubrique SNS souhaitée. (Vous pouvez vous abonner à plusieurs files d'attente d'une rubrique SNS.) Pour plus d'informations, consultez Envoi de messages d'Amazon SNS aux files d'attente Amazon SQS.

Autorisations pour Amazon SQS

Pour utiliser Amazon SQS avec AWS Config, vous devez configurer une politique qui accorde des autorisations à votre compte pour effectuer toutes les actions autorisées sur une file d'attente SQS. L'exemple de stratégie suivant accorde au numéro de compte 111122223333 et au numéro de compte 444455556666 la permission d'envoyer des messages se rapportant à chaque changement de configuration dans la file d'attente nommée arn:aws:sqs:us-east-2:444455556666:queue1.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

Vous devez également créer une stratégie qui accorde des autorisations pour les connexions entre une rubrique SNS et la file d'attente SQS qui souscrit à cette rubrique. Voici un exemple de politique qui permet à la rubrique SNS portant le nom de ressource Amazon (ARN) arn:aws:sns:us-east-2:111122223333:test-topic d'effectuer des actions sur la file d'attente nommée arn:aws:sqs:us-east-2:111122223333 :. test-topic-queue

> **Note**
>
> Le compte de la rubrique SNS et la file d'attente SQS doivent être dans la même région.

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Chaque stratégie peut inclure des instructions qui couvrent uniquement une seule file d'attente, et non plusieurs files d'attente. Pour plus d'informations sur les autres restrictions sur les politiques Amazon SQS, consultez Informations spéciales relatives aux politiques Amazon SQS.

Surveillance AWS Config avec Amazon EventBridge

Amazon EventBridge fournit un flux d'événements système en temps quasi réel qui décrivent les modifications apportées aux AWS ressources. Utilisez Amazon EventBridge pour détecter les changements de statut des AWS Config événements et y réagir.

Vous pouvez créer une règle qui s'exécute à chaque changement de statut ou lorsqu'un ou plusieurs statuts spécifiques sont activés. Ensuite, en fonction des règles que vous créez, Amazon EventBridge invoque une ou plusieurs actions cibles lorsqu'un événement correspond aux valeurs que vous spécifiez dans une règle. En fonction du type d’événement, vous pouvez envoyer des notifications, capturer les informations sur l’événement, prendre des mesures correctives, déclencher des événements ou prendre d’autres mesures.

Avant de créer des règles d'événement pour AWS Config, toutefois, vous devez effectuer les opérations suivantes :

- Familiarisez-vous avec les événements, les règles et les cibles dans EventBridge. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EventBridge ?
- Pour plus d'informations sur la prise en main EventBridge et la configuration des règles, consultez Getting started with Amazon EventBridge.
- Créez la ou les cible(s), que vous allez utiliser dans vos règles d'événement.

Rubriques

- EventBridge Format Amazon pour AWS Config
- Création d'une EventBridge règle Amazon pour AWS Config

EventBridge Format Amazon pour AWS Config

L' EventBridge événement pour AWS Config a le format suivant :

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

Création d'une EventBridge règle Amazon pour AWS Config

Suivez les étapes ci-dessous pour créer une EventBridge règle qui se déclenche sur un événement émis par AWS Config. Les événements sont générés dans la mesure du possible.

1. Dans le volet de navigation, choisissez Règles.
2. Choisissez Créer une règle.

3. Saisissez un nom et une description pour la règle.

   Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.

4. Pour Type de règle, choisissez Règle avec un modèle d'événement.
5. Dans Source de l'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
6. (Facultatif) Pour Type d'exemple d'événement, choisissez Événements AWS .
7. Pour Exemple d'événements, choisissez le type d'événement qui déclenche la règle :
   - Choisissez AWS API Call via CloudTrail pour baser les règles sur les appels d'API effectués vers ce service. Pour plus d'informations sur la création de ce type de règle, consultez Tutoriel : Création d'une EventBridge règle Amazon pour les appels AWS CloudTrail d'API.
   - Choisissez Config Configuration Item Change pour recevoir des notifications lorsqu'une ressource de votre compte est modifiée.

     Comme décrit dans ces articles d'assistance, vous pouvez utiliser EventBridge pour recevoir des notifications par e-mail personnalisées lorsqu'une ressource est créée ou supprimée. Comment puis-je recevoir des notifications par e-mail personnalisées lorsqu'une ressource est créée dans mon AWS Config service Compte AWS d'utilisation ? et Comment puis-je recevoir des notifications par e-mail personnalisées lorsqu'une ressource est supprimée dans mon AWS Config service Compte AWS d'utilisation ? .
   - Choisissez Config Rules Compliance Change pour recevoir des notifications lorsqu'une vérification de conformité de vos règles échoue.

     Comme décrit dans cet article de support, vous pouvez utiliser EventBridge pour recevoir des notifications par e-mail personnalisées lorsqu'une ressource n'est pas conforme. Comment puis-je être averti lorsqu'une AWS ressource n'est pas conforme en utilisant ? AWS Config.
   - Choisissez Config Rules Re-evaluation Status pour recevoir des notifications de statut de réévaluation.
   - Choisissez Config Configuration Snapshot Delivery Status pour recevoir des notifications du statut de diffusion d'un instantané de configuration.
   - Choisissez Config Configuration History Delivery Status pour recevoir des notifications du statut de diffusion d'un historique de configuration.
8. Pour la Méthode de création, choisissez Utiliser le formulaire de modèle.
9. Pour Source d'événement, choisissez Services AWS .

10. Pour le Service AWS , choisissez Config.

11. Pour Type d'événement, choisissez le type d'événement qui déclenche la règle :

- Choisissez Tous les événements pour établir une règle qui s'applique à tous les AWS services. Si vous choisissez cette option, vous ne pouvez pas choisir les types de messages spécifiques, les noms de règle, les types de ressource ou les ID de ressource.
- Choisissez AWS API Call via CloudTrail pour baser les règles sur les appels d'API effectués vers ce service. Pour plus d'informations sur la création de ce type de règle, consultez Tutoriel : Création d'une EventBridge règle Amazon pour les appels AWS CloudTrail d'API.
- Choisissez Config Configuration Item Change pour recevoir des notifications lorsqu'une ressource de votre compte est modifiée.

  Comme décrit dans ces articles d'assistance, vous pouvez utiliser EventBridge pour recevoir des notifications par e-mail personnalisées lorsqu'une ressource est créée ou supprimée. Comment puis-je recevoir des notifications par e-mail personnalisées lorsqu'une ressource est créée dans mon AWS Config service Compte AWS d'utilisation ? et Comment puis-je recevoir des notifications par e-mail personnalisées lorsqu'une ressource est supprimée dans mon AWS Config service Compte AWS d'utilisation ? .
- Choisissez Config Rules Compliance Change pour recevoir des notifications lorsqu'une vérification de conformité de vos règles échoue.

  Comme décrit dans cet article de support, vous pouvez utiliser EventBridge pour recevoir des notifications par e-mail personnalisées lorsqu'une ressource n'est pas conforme. Comment puis-je être averti lorsqu'une AWS ressource n'est pas conforme en utilisant ? AWS Config.
- Choisissez Config Rules Re-evaluation Status pour recevoir des notifications de statut de réévaluation.
- Choisissez Config Configuration Snapshot Delivery Status pour recevoir des notifications du statut de diffusion d'un instantané de configuration.
- Choisissez Config Configuration History Delivery Status pour recevoir des notifications du statut de diffusion d'un historique de configuration.

12. Choisissez Tout type de message pour recevoir des notifications de tout type. Choisissez Type(s) de message spécifique(s) pour recevoir les types de notification suivants :

- Si vous le souhaitez ConfigurationItemChangeNotification, vous recevez des messages lorsque la configuration d'une ressource qui AWS Config évalue a changé.
- Si vous choisissez ComplianceChangeNotification, vous recevez des messages lorsque le type de conformité d'une ressource AWS Config évaluant a changé.

- Si vous le souhaitez ConfigRulesEvaluationStarted, vous recevez des messages lorsque vous AWS Config commencez à évaluer votre règle par rapport aux ressources spécifiées.
- Si vous le souhaitez ConfigurationSnapshotDeliveryCompleted, vous recevez des messages lorsque l'instantané de configuration est AWS Config correctement envoyé à votre compartiment Amazon S3.
- Si vous le souhaitez ConfigurationSnapshotDeliveryFailed, vous recevez des messages lorsque vous AWS Config ne parvenez pas à fournir l'instantané de configuration à votre compartiment Amazon S3.
- Si vous le souhaitez ConfigurationSnapshotDeliveryStarted, vous recevez des messages lorsque AWS Config vous commencez à envoyer l'instantané de configuration à votre compartiment Amazon S3.
- Si vous le souhaitez ConfigurationHistoryDeliveryCompleted, vous recevez des messages lorsque l'historique de configuration est AWS Config correctement transmis à votre compartiment Amazon S3.

13. Si vous avez choisi un type d'événement spécifique dans la liste déroulante Type d'événement, choisissez N'importe quel type de ressource pour établir une règle qui s'applique à tous les types de ressources AWS Config pris en charge.

    Vous pouvez aussi choisir Type(s) de ressource spécifique(s), puis saisir le type de ressource pris en charge par AWS Config (par exemple, `AWS::EC2::Instance`).

14. Si vous choisissez un type d'événement spécifique dans la liste déroulante Type d'événement, choisissez N'importe quel ID de ressource pour inclure tous les ID de ressource pris en charge par AWS Config .

    Vous pouvez aussi choisir ID de ressource spécifique(s), puis saisir l'ID de ressource pris en charge par AWS Config (par exemple, `i-04606de676e635647`).

15. Si vous choisissez un type d'événement spécifique dans la liste déroulante Type d'événement, choisissez Tout nom de règle pour inclure toutes les règles prises en charge par AWS Config .

    Vous pouvez aussi choisir Nom(s) de règle spécifique(s), puis saisir la règle prise en charge par AWS Config (par exemple, required-tags).

16. Pour Sélectionner une ou plusieurs cibles, choisissez le type de cible que vous avez préparé pour l'utiliser avec cette règle, puis configurez les options supplémentaires requises par ce type de cible.

17. Les champs affichés varient en fonction du service que vous choisissez. Entrez les informations spécifiques requises pour ce type de cible.
18. Pour de nombreux types de cibles, EventBridge nécessite des autorisations pour envoyer des événements à la cible. Dans ces cas, EventBridge vous pouvez créer le rôle IAM nécessaire à l'exécution de votre règle.
    - Pour créer un rôle IAM automatiquement, sélectionnez Create a new role for this specific resource.
    - Pour utiliser un rôle IAM que vous avez créé auparavant, sélectionnez Use existing role (Utiliser un rôle existant).
19. (Facultatif) Sélectionnez Ajouter une cible pour ajouter une autre cible pour cette règle.
20. (Facultatif) Saisissez une ou plusieurs balises pour la règle. Pour plus d'informations, consultez Amazon EventBridge tags.
21. Passez en revue la configuration de votre règle pour vous assurer qu'elle correspond à vos besoins de surveillance des événements.
22. Choisissez Créer pour confirmer votre sélection.

Utilisation AWS Config avec Interface Amazon VPC Endpoints

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez établir une connexion privée entre votre VPC et. AWS Config Vous pouvez utiliser cette connexion pour communiquer avec AWS Config à partir de votre VPC sans passer par le réseau Internet public.

Amazon VPC est un AWS service que vous pouvez utiliser pour lancer AWS des ressources dans un réseau virtuel que vous définissez. Avec un VPC, vous contrôlez des paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles réseau. Les points de terminaison VPC d'interface sont alimentés par AWS PrivateLink une AWS technologie qui permet une communication privée entre les AWS services à l'aide d'une interface Elastic Network avec des adresses IP privées. Pour connecter votre VPC à AWS Config, vous définissez un point de terminaison VPC d'interface pour. AWS Config Ce type de point de terminaison vous permet de connecter votre VPC à AWS des services. Le point de terminaison fournit une connectivité fiable et évolutive AWS Config sans nécessiter de passerelle Internet, d'instance de traduction d'adresses réseau (NAT) ou de connexion VPN. Pour de plus amples informations, consultez Qu'est-ce qu'Amazon VPC ? dans le Guide de l'utilisateur Amazon VPC.

Les étapes suivantes s'adressent aux utilisateurs d'Amazon VPC. Pour plus d'informations, consultez Démarrez dans le Amazon VPC Guide de l'utilisateur.

Créez un point de terminaison VPC pour AWS Config

Pour commencer à utiliser AWS Config avec votre VPC, créez un point de terminaison VPC d'interface pour. AWS Config Il n'est pas nécessaire de modifier les paramètres de AWS Config. AWS Config appelle d'autres AWS services en utilisant leurs points de terminaison publics. Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Amazon VPC Guide de l'utilisateur.

Questions fréquentes (FAQ)

Impossible de voir mes dernières modifications de configuration

Puis-je m'attendre à voir mes modifications de configuration immédiatement ?

AWS Config enregistre généralement les modifications de configuration de vos ressources juste après la détection d'une modification, ou à la fréquence que vous spécifiez. Cependant, cela se fait dans la mesure du possible et peut parfois prendre plus de temps. Si les problèmes persistent après un certain temps, contactez AWS Supportet fournissez vos AWS Config statistiques prises en charge par Amazon CloudWatch. Pour plus d'informations sur ces mesures, consultez la section Mesures AWS Config d'utilisation et de réussite.

Relations indirectes dans AWS Config

Rubriques

- Qu'est-ce que la relation entre les ressources ?
- Que sont les relations directes et indirectes entre les ressources ?
- Quelles sont les relations indirectes prises AWS Config en charge ?
- Comment les éléments de configuration sont-ils créés en cas de relation directe et indirecte ?
- Quels sont les éléments de configuration générés par les relations indirectes ?
- Comment récupérer les données de configuration liées aux relations indirectes ?

Qu'est-ce que la relation entre les ressources ?

Dans AWS, les ressources font référence à des entités gérables, telles qu'une instance Amazon Elastic Compute Cloud (Amazon EC2), une AWS CloudFormation pile ou un bucket Amazon S3. AWS Config est un service qui suit et surveille les ressources en créant des éléments de configuration (CI) chaque fois qu'une modification d'un type de ressource enregistrée est détectée, ou à la fréquence d'enregistrement que vous avez définie. Par exemple, lorsqu'il AWS Config est configuré pour suivre les instances Amazon EC2, il crée un élément de configuration chaque fois qu'une instance est créée, mise à jour ou supprimée. Chaque élément de configuration créé par AWS Config comporte plusieurs champs`accountId`, notamment `arn` (Amazon Resource

Name)`awsRegion`,`configuration`,`tags`, et`relationships`. Le champ de relations d'un CI permet d' AWS Config afficher comment les ressources sont liées les unes aux autres. Par exemple, une relation peut indiquer qu'un volume Amazon EBS présentant l'ID `vol-123ab45d` est attaché à une instance Amazon EC2 présentant l'ID `i-a1b2c3d4`, elle-même associée au groupe de sécurité `sg-ef678hk`.

Que sont les relations directes et indirectes entre les ressources ?

AWS Config déduit les relations pour la plupart des types de ressources à partir du champ de configuration, appelées relations « directes ». Une relation directe est une connexion unidirectionnelle (A→B) entre une ressource (A) et une autre ressource (B), généralement obtenue à partir de la réponse de description de l'API de la ressource (A). Dans le passé, pour certains types de ressources AWS Config initialement pris en charge, il capturait également les relations issues des configurations d'autres ressources, créant ainsi des relations « indirectes » bidirectionnelles (B→A). Par exemple, la relation entre une instance Amazon EC2 et son groupe de sécurité est directe car les groupes de sécurité sont inclus dans la réponse de description de l'API pour l'instance Amazon EC2. D'autre part, la relation entre un groupe de sécurité et une instance Amazon EC2 est indirecte car la description d'un groupe de sécurité ne renvoie aucune information sur les instances auxquelles il est associé. Par conséquent, lorsqu'un changement de configuration de ressource est détecté, AWS Config crée non seulement un CI pour cette ressource, mais génère également des CI pour toutes les ressources associées, y compris celles présentant des relations indirectes. Par exemple, lorsqu'il AWS Config détecte des modifications dans une instance Amazon EC2, il crée un CI pour l'instance et un CI pour le groupe de sécurité associé à l'instance.

Quelles sont les relations indirectes prises AWS Config en charge ?

Les relations de ressources indirectes suivantes sont prises en charge dans AWS Config.

Type de ressource	est indirectement lié au type de ressource		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` ,		

Type de ressource	est indirectement lié au type de ressource		
	AWS::EC2::VPNGateway , AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		

Type de ressource	est indirectement lié au type de ressource		
`AWS::EC2::SecurityGroup`	`AWS::EC2::VPC`		
`AWS::EC2::Subnet`	`AWS::EC2::VPC`		
`AWS::EC2::VPNGateway`	`AWS::EC2::VPC`		

Comment les éléments de configuration sont-ils créés en cas de relation directe et indirecte ?

Pour une relation directe entre les ressources (A→B), tout changement de configuration apporté à la ressource B générera également un élément de configuration (CI) pour la ressource A. De même, pour une relation indirecte (B→A), lorsqu'un changement de configuration est apporté à la ressource A, un nouveau CI est généré pour la ressource B. Par exemple, l'instance Amazon EC2 avec le groupe de sécurité est une relation directe, de sorte que tout changement de configuration apporté à un groupe de sécurité générerait un CI pour le groupe de sécurité ainsi qu'un CI pour l'instance EC2. De même, le groupe de sécurité et l'instance Amazon EC2 constituent une relation indirecte, de sorte que tout changement de configuration apporté à une instance EC2 générera un CI pour l'instance Amazon EC2 ainsi qu'un CI pour le groupe de sécurité.

Quels sont les éléments de configuration générés par les relations indirectes ?

Vous trouverez ci-dessous les éléments de configuration supplémentaires (CI) générés en cas de relations de indirectes entre les ressources.

Des changements de configuration sont apportés aux types de ressources suivants	générera des CI pour les types de ressources suivants		
AWS::EC2::RouteTable	AWS::EC2::Instance , AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , et AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

Des changements de configuration sont apportés aux types de ressources suivants	générera des CI pour les types de ressources suivants		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

Comment récupérer les données de configuration liées aux relations indirectes ?

Vous pouvez exécuter des requêtes SQL (Structured Query Language) dans les requêtes AWS Config avancées pour récupérer les données de configuration relatives aux relations de ressources indirectes. Si vous souhaitez par exemple récupérer la liste des instances Amazon EC2 associées à un groupe de sécurité, utilisez la requête suivante :

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
```

```
    relationships.resourceId = 'sg-234213'
```

Exemples de code pour AWS Config l'utilisation des AWS SDK

Les exemples de code suivants montrent comment utiliser AWS Config un kit de développement AWS logiciel (SDK).

Les actions sont des extraits de code de programmes plus larges et doivent être exécutées dans leur contexte. Alors que les actions vous indiquent comment appeler des fonctions de service individuelles, vous pouvez les voir en contexte dans leurs scénarios associés et dans des exemples interservices.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes du kit de développement logiciel (SDK).

Exemples de code

- Actions relatives à AWS Config l'utilisation des AWS SDK
  - Utilisation DeleteConfigRule avec un AWS SDK ou une CLI
  - Utilisation DescribeComplianceByConfigRule avec un AWS SDK ou une CLI
  - Utilisation DescribeComplianceByResource avec un AWS SDK ou une CLI
  - Utilisation DescribeConfigRuleEvaluationStatus avec un AWS SDK ou une CLI
  - Utilisation DescribeConfigRules avec un AWS SDK ou une CLI
  - Utilisation DescribeConfigurationRecorderStatus avec un AWS SDK ou une CLI
  - Utilisation DescribeConfigurationRecorders avec un AWS SDK ou une CLI
  - Utilisation DescribeDeliveryChannels avec un AWS SDK ou une CLI
  - Utilisation GetComplianceDetailsByConfigRule avec un AWS SDK ou une CLI
  - Utilisation GetComplianceDetailsByResource avec un AWS SDK ou une CLI
  - Utilisation GetComplianceSummaryByConfigRule avec un AWS SDK ou une CLI
  - Utilisation GetComplianceSummaryByResourceType avec un AWS SDK ou une CLI
  - Utilisation PutConfigRule avec un AWS SDK ou une CLI
  - Utilisation PutDeliveryChannel avec un AWS SDK ou une CLI

Actions relatives à AWS Config l'utilisation des AWS SDK

Les exemples de code suivants montrent comment effectuer des AWS Config actions individuelles avec AWS les SDK. Ces extraits appellent l' AWS Config API et sont des extraits de code de programmes plus volumineux qui doivent être exécutés en contexte. Chaque exemple inclut un lien vers GitHub, où vous pouvez trouver des instructions pour configurer et exécuter le code.

Les exemples suivants incluent uniquement les actions les plus couramment utilisées. Pour obtenir la liste complète, veuillez consulter la AWS Config Référence d'API.

Exemples

- Utilisation DeleteConfigRule avec un AWS SDK ou une CLI
- Utilisation DescribeComplianceByConfigRule avec un AWS SDK ou une CLI
- Utilisation DescribeComplianceByResource avec un AWS SDK ou une CLI
- Utilisation DescribeConfigRuleEvaluationStatus avec un AWS SDK ou une CLI
- Utilisation DescribeConfigRules avec un AWS SDK ou une CLI
- Utilisation DescribeConfigurationRecorderStatus avec un AWS SDK ou une CLI
- Utilisation DescribeConfigurationRecorders avec un AWS SDK ou une CLI
- Utilisation DescribeDeliveryChannels avec un AWS SDK ou une CLI
- Utilisation GetComplianceDetailsByConfigRule avec un AWS SDK ou une CLI
- Utilisation GetComplianceDetailsByResource avec un AWS SDK ou une CLI
- Utilisation GetComplianceSummaryByConfigRule avec un AWS SDK ou une CLI
- Utilisation GetComplianceSummaryByResourceType avec un AWS SDK ou une CLI
- Utilisation PutConfigRule avec un AWS SDK ou une CLI
- Utilisation PutDeliveryChannel avec un AWS SDK ou une CLI

Utilisation `DeleteConfigRule` avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DeleteConfigRule`.

CLI

AWS CLI

Pour supprimer une règle AWS Config

La commande suivante supprime une règle AWS Config nommée `MyConfigRule` :

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Pour plus de détails sur l'API, reportez-vous DeleteConfigRuleà la section Référence des AWS CLI commandes.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Pour plus de détails sur l'API, consultez DeleteConfigRulele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeComplianceByConfigRule`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeComplianceByConfigRule`.

CLI

AWS CLI

Pour obtenir des informations de conformité pour vos règles de AWS Config

La commande suivante renvoie des informations de conformité pour chaque règle de AWS Config violée par une ou plusieurs AWS ressources :

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de ressources qui ne sont pas conformes à la règle correspondante. Par exemple, le résultat suivant indique que 3 ressources ne sont pas conformes à la règle nommée`InstanceTypesAreT2micro`.

Sortie :

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
```

```
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByConfigRuleà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple récupère les détails de conformité de la règle ebs-optimized-instance, pour laquelle il n'existe aucun résultat d'évaluation actuel pour la règle, il renvoie donc INSUFFIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Sortie :

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Exemple 2 : Cet exemple renvoie le nombre de ressources non conformes pour la règle ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Sortie :

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByConfigRuleà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeComplianceByResource`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeComplianceByResource`.

CLI

AWS CLI

Pour obtenir des informations de conformité pour vos AWS ressources

La commande suivante renvoie des informations de conformité pour chaque instance EC2 enregistrée par AWS Config et qui enfreint une ou plusieurs règles :

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Dans le résultat, la valeur de chaque `CappedCount` attribut indique le nombre de règles violées par la ressource. Par exemple, le résultat suivant indique que l'instance `i-1a2b3c4d` enfreint 2 règles.

Sortie :

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByResourceà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple vérifie le type de **`AWS::SSM::ManagedInstanceInventory`** ressource pour le type de conformité « COMPLIANT ».

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Sortie :

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Pour plus de détails sur l'API, reportez-vous DescribeComplianceByResourceà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeConfigRuleEvaluationStatus`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeConfigRuleEvaluationStatus`.

CLI

AWS CLI

Pour obtenir les informations d'état d'une règle AWS Config

La commande suivante renvoie les informations d'état d'une règle AWS Config nommée `MyConfigRule` :

```
aws configservice describe-config-rule-evaluation-status --config-rule-names
 MyConfigRule
```

Sortie :

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
```

```
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigRuleEvaluationStatusà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie les informations d'état pour les règles de configuration données.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Sortie :

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
```

```
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigRuleEvaluationStatusà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeConfigRules`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeConfigRules`.

CLI

AWS CLI

Pour obtenir les détails d'une règle AWS Config

La commande suivante renvoie les détails d'une règle AWS Config nommée `InstanceTypesAreT2micro` :

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

Sortie :

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
```

```
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigRulesà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple répertorie les règles de configuration du compte, avec les propriétés sélectionnées.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Sortie :

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                      ------------
 -------------
 ---------------
```

```
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigRulesà la section Référence des AWS Tools for PowerShell applets de commande.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
```

```
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Pour plus de détails sur l'API, consultez DescribeConfigRulesle AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeConfigurationRecorderStatus`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeConfigurationRecorderStatus`.

CLI

AWS CLI

Pour obtenir des informations d'état pour l'enregistreur de configuration

La commande suivante renvoie l'état de l'enregistreur de configuration par défaut :

```
aws configservice describe-configuration-recorder-status
```

Sortie :

```
{
```

```
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigurationRecorderStatusà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie l'état des enregistreurs de configuration.

```
Get-CFGConfigurationRecorderStatus
```

Sortie :

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigurationRecorderStatusà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeConfigurationRecorders`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeConfigurationRecorders`.

CLI

AWS CLI

Pour obtenir des informations sur l'enregistreur de configuration

La commande suivante renvoie des informations sur l'enregistreur de configuration par défaut :

```
aws configservice describe-configuration-recorders
```

Sortie :

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigurationRecordersà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie les détails des enregistreurs de configuration.

```
Get-CFGConfigurationRecorder | Format-List
```

Sortie :

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Pour plus de détails sur l'API, reportez-vous DescribeConfigurationRecordersà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`DescribeDeliveryChannels`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`DescribeDeliveryChannels`.

CLI

AWS CLI

Pour obtenir des informations sur le canal de livraison

La commande suivante renvoie des informations sur le canal de diffusion :

```
aws configservice describe-delivery-channels
```

Sortie :

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
```

```
}
```

- Pour plus de détails sur l'API, reportez-vous DescribeDeliveryChannelsà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple extrait le canal de distribution de la région et affiche les détails.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Sortie :

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Pour plus de détails sur l'API, reportez-vous DescribeDeliveryChannelsà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetComplianceDetailsByConfigRule`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Pour obtenir les résultats de l'évaluation d'une règle AWS Config

La commande suivante renvoie les résultats de l'évaluation pour toutes les ressources qui ne sont pas conformes à une règle de AWS configuration nommée `InstanceTypesAreT2micro` :

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Sortie :

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
```

```
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByConfigRuleà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple obtient les résultats de l'évaluation de la règle access-keys-rotated et renvoie la sortie groupée par type de conformité

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Sortie :

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Exemple 2 : Cet exemple interroge les détails de conformité de la règle relative access-keys-rotated aux ressources COMPLIANT.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Sortie :

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByConfigRuleà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetComplianceDetailsByResource`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetComplianceDetailsByResource`.

CLI

AWS CLI

Pour obtenir les résultats de l'évaluation d'une AWS ressource

La commande suivante renvoie les résultats de l'évaluation pour chaque règle à laquelle l'instance EC2 n'est `i-1a2b3c4d` pas conforme :

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Sortie :

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
```

```
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByResourceà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple d'évaluation donne des résultats pour la ressource donnée.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Sortie :

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
```

```
ResultToken                :
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceDetailsByResourceà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetComplianceSummaryByConfigRule`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Pour obtenir le résumé de conformité de vos règles de AWS Config

La commande suivante renvoie le nombre de règles conformes et le nombre de règles non conformes :

```
aws configservice get-compliance-summary-by-config-rule
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de règles conformes ou non conformes.

Sortie :

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
```

```
        }
    }
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByConfigRuleà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie le nombre de règles Config non conformes.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Sortie :

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByConfigRuleà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`GetComplianceSummaryByResourceType`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Pour obtenir le résumé de conformité pour tous les types de ressources

La commande suivante renvoie le nombre de AWS ressources non conformes et le nombre de ressources conformes :

```
aws configservice get-compliance-summary-by-resource-type
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de ressources conformes ou non conformes.

Sortie :

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Pour obtenir le résumé de conformité pour un type de ressource spécifique

La commande suivante renvoie le nombre d'instances EC2 non conformes et le nombre d'instances conformes :

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

Dans la sortie, la valeur de chaque `CappedCount` attribut indique le nombre de ressources conformes ou non conformes.

Sortie :

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByResourceTypeà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple renvoie le nombre de ressources conformes ou non conformes et convertit la sortie en json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
```

```
}
```

- Pour plus de détails sur l'API, reportez-vous GetComplianceSummaryByResourceTypeà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`PutConfigRule`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`PutConfigRule`.

CLI

AWS CLI

Pour ajouter une règle Config AWS gérée

La commande suivante fournit du code JSON pour ajouter une règle de configuration AWS gérée :

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json`est un fichier JSON qui contient la configuration des règles :

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
```

```
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Pour l'`ComplianceResourceTypes`attribut, ce code JSON limite la portée aux ressources de ce `AWS::EC2::Instance` type. AWS Config évaluera donc uniquement les instances EC2 par rapport à la règle. Comme la règle est une règle gérée, l'`Owner`attribut est défini sur`AWS`, et l'`SourceIdentifier`attribut est défini sur l'identifiant de règle,`REQUIRED_TAGS`. Pour l'`InputParameters`attribut, les clés de balise requises par la règle, `CostCenter` et`Owner`, sont spécifiées.

Si la commande aboutit, AWS Config ne renvoie aucune sortie. Pour vérifier la configuration des règles, exécutez la describe-config-rules commande et spécifiez le nom de la règle.

Pour ajouter une règle Config gérée par le client

La commande suivante fournit du code JSON pour ajouter une règle de configuration gérée par le client :

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json`est un fichier JSON qui contient la configuration des règles :

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
```

```
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Pour l'`ComplianceResourceTypes`attribut, ce code JSON limite la portée aux ressources de ce `AWS::EC2::Instance` type. AWS Config évaluera donc uniquement les instances EC2 par rapport à la règle. Cette règle étant une règle gérée par le client, l'`Owner`attribut est défini sur`CUSTOM_LAMBDA`, et l'`SourceIdentifier`attribut est défini sur l'ARN de la fonction AWS Lambda. L'`SourceDetails`objet est obligatoire. Les paramètres spécifiés pour l'`InputParameters`attribut sont transmis à la fonction AWS Lambda lorsque AWS Config l'invoque pour évaluer les ressources par rapport à la règle.

Si la commande aboutit, AWS Config ne renvoie aucune sortie. Pour vérifier la configuration des règles, exécutez la describe-config-rules commande et spécifiez le nom de la règle.

- Pour plus de détails sur l'API, reportez-vous PutConfigRuleà la section Référence des AWS CLI commandes.

Python

SDK pour Python (Boto3)

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
```

```
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Pour plus de détails sur l'API, consultez PutConfigRulele AWS manuel de référence de l'API SDK for Python (Boto3).

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Utilisation **`PutDeliveryChannel`** avec un AWS SDK ou une CLI

Les exemples de code suivants montrent comment utiliser`PutDeliveryChannel`.

CLI

AWS CLI

Pour créer un canal de diffusion

La commande suivante fournit les paramètres du canal de diffusion sous forme de code JSON :

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

Le `deliveryChannel.json` fichier spécifie les attributs du canal de diffusion :

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Cet exemple définit les attributs suivants :

`name`- Le nom du canal de diffusion. Par défaut, AWS Config attribue le nom `default` à un nouveau canal de distribution. Vous ne pouvez pas mettre à jour le nom du canal de distribution avec la commande. `put-delivery-channel` Pour connaître les étapes à suivre pour modifier le nom, voir Renommer le canal de diffusion. `s3BucketName` - Le nom du compartiment Amazon S3 auquel AWS Config fournit des instantanés de configuration et des fichiers d'historique de configuration. Si vous spécifiez un compartiment appartenant à un autre AWS compte, ce compartiment doit disposer de politiques accordant des autorisations d'accès à Config. AWS Pour de plus d'informations, consultez Autorisations pour le compartiment Amazon S3.

`snsTopicARN`- Le nom de ressource Amazon (ARN) de la rubrique Amazon SNS à laquelle AWS Config envoie des notifications concernant les modifications de configuration. Si vous choisissez un sujet depuis un autre compte, le sujet doit comporter des politiques accordant des autorisations d'accès à Config. AWS Pour plus d'informations, consultez la rubrique Autorisations pour Amazon SNS.

`configSnapshotDeliveryProperties`- Contient l'`deliveryFrequency`attribut, qui définit la fréquence à laquelle AWS Config fournit des instantanés de configuration et la fréquence à laquelle il invoque des évaluations pour les règles de configuration périodiques.

Si la commande aboutit, AWS Config ne renvoie aucune sortie. Pour vérifier les paramètres de votre canal de diffusion, exécutez la describe-delivery-channels commande.

- Pour plus de détails sur l'API, reportez-vous PutDeliveryChannelà la section Référence des AWS CLI commandes.

PowerShell

Outils pour PowerShell

Exemple 1 : Cet exemple modifie la propriété DeliveryFrequency d'un canal de diffusion existant.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Pour plus de détails sur l'API, reportez-vous PutDeliveryChannelà la section Référence des AWS Tools for PowerShell applets de commande.

Pour obtenir la liste complète des guides de développement du AWS SDK et des exemples de code, consultezUtilisation AWS Config avec un AWS SDK. Cette rubrique comprend également des informations sur le démarrage et sur les versions précédentes de SDK.

Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation de AWS Config. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

- Version de l'API : 2014-11-12
- Dernière mise à jour de la documentation : 17 juin 2024

Modification	Description	Date
Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Elastic File System (Amazon EFS), Amazon Redshift et. Gestionnaire de systèmes AWS pour SAP Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	17 juin 2024
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • accès public à cloudtrail-s3-bucket interdit • journalisation de l'accès au compartiment 3 dans le cloud trail	8 mai 2024
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge la	2 mai 2024

	règle gérée suivante : iam-external-access-analyzer-enabled	
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • activé par guardduty-malware-protection • guardduty-rds-protection activé • protection guardduty-S3 activée • inspector-lambda compatible avec le scan standard	26 avril 2024

AWS Config simplifie l'analyse de l'utilisation avec Amazon CloudWatch	Dans cette version, les CloudWatch statistiques Amazon relatives au suivi de l'utilisation AWS Config des données n'afficheront que l'utilisation facturabl e. Cela signifie que l'utilisa tion non facturable ne sera plus affichée à la fois dans les CloudWatch métriques Amazon émises AWS Config et dans la AWS Config console. Cela vous permet de valider la AWS Config configuration et l'utilisation à l'aide CloudWatch des statistiques Amazon et de corréler l'utilisation facturabl e aux coûts associés. Pour plus d'informations, consultez la section Indicateurs AWS Config d'utilisation et de réussite.	26 avril 2024
AWS Config met à jour les règles gérées	Cette version AWS Config prend en charge la règle gérée suivante : iam-server-certifi cate-expiration-check	23 avril 2024

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • contrôle des restrictions de port vpc-sg- • vérification des événements de données cloudtrail-all-write-s3 • Cloudtrail-all-read-s3-data-event-check	17 avril 2024
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • guardduty-eks-protection-audit activé • guardduty-eks-protection-runtime activé • compatible avec la protection GuardDuty-Lambda • compatible avec inspector-ec2-scan • compatible avec inspector-ecr-scan • compatible avec le scan de code inspector-lambda • accès au port non restreint par redshift	16 avril 2024
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge la règle gérée suivante : efs-mount-target-public-accessible	20 mars 2024

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • Autorisation DMS-NEPTUNE-IAM activée • Authentification DMS-MONGO-DB activée • compatible DMS-REDIS-TLS • chiffrement des points de terminaison dax-tls • eks-cluster-secrets-encrypted • Kinesis-Firehose Delivery-Stream crypté • compatible avec mq-cloudwatch-audit-log • compatible avec mq-cloudwatch-audit-log • opensearch-primary-node-fault-tolerance • sagemaker-endpoint-config-prod-instance-count • catalogue de services partagé au sein de l'organisation • transfer-family-server-no-ftp	26 février 2024

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Managed Service pour Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, Amazon AWS Glue FSx ElastiCache, (IAM) AWS Identity and Access Management ,,, Amazon Redshift Serverless AWS Lambda AWS RAM, Amazon et Amazon Simple Notification Service (SageMakerAmazon SNS). Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	22 février 2024
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge la règle gérée suivante : s3-bucket-cross-region-replication-enabled	12 février 2024

AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modificat ions de configuration apportées AWS Config aux nouveaux types de ressources AWS AppConfig , Amazon CloudWatch Evidently AWS Identity and Access Management (IAM), Amazon MemoryDB pour Redis (MemoryDB), Amazon Managed Streaming pour Apache Kafka (Amazon MSK), Amazon Redshift et autres types de ressources. AWS Transfer Family Pour plus d'informations, consultez Types de ressources pris en charge.	6 février 2024
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge la règle gérée suivante : macie-auto-sensitive-data-discovery-check	29 janvier 2024

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les AWS Config modifications de configuration apportées aux nouveaux Amazon AppStream , AWS Key Managemen t Service (AWS KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon EC2), EC2 Image Builder, QuickSight Amazon AWS Ground Station AWS Mainframe Modernization, Amazon Redshift et aux types de ressources. AWS Systems Manager Pour plus d'informa tions, consultez Types de ressources pris en charge.	3 janvier 2024

Les limites de service augmentent jusqu'au nombre maximum de AWS Config règles par région et par compte	Cette version AWS Config prend en charge 1 000 AWS Config règles par AWS région et par compte. Cette augmentation s'applique au total de toutes les règles déployées, y compris les règles AWS Config gérées, les règles AWS Config personnalisées, les packs de AWS Config conformité, les AWS Security Hub contrôles, AWS Firewall Manager les politiques et les plans de AWS Backup sauvegarde par région et par compte. Pour plus d'informations, consultez Limites de service .	19 décembre 2023

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • s3-meets-restore-time-target • ebs-meets-restore-time-target • ec2-meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	19 décembre 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM, Amazon Managed Streaming for Apache Kafka AWS Identity and Access Management(Amazon MSK) AWS Organizations, Amazon Logs et CloudWatch Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	5 décembre 2023

Version préliminaire : processeur de requêtes en langage naturel pour les requêtes avancées	Dans cette version, vous pouvez utiliser le processeur de requêtes en langage naturel pour les requêtes avancées, qui utilise des fonctionnalités d'intelligence artificielle générative (IA générative) qui vous permettent de poser des questions en anglais simple et de les convertir dans un format de ready-to-use requête. Avec le processeur de requêtes en langage naturel, vous pouvez interroger votre organisation Compte AWS ou l'ensemble d'une AWS organisation. Pour plus d’informations, consultez Processeur de requêtes en langage naturel pour les requêtes avancées.	26 novembre 2023

Enregistrement périodique	Avec cette version, AWS Config prend en charge l'enregistrement périodique. L'enregistrement périodique vous permet de capturer les dernières modifications de configuration de vos ressources sur une période de temps déterminée. Vous pouvez désormais configurer la fréquence par défaut de l'enregistreur de configuration de manière à recevoir un élément de configuration représentant l'état le plus récent de vos ressources au cours des dernières 24 heures, uniquement s'il est différent de l'élément de configuration enregistré précédemment. La AWS Config console introduit également une nouvelle expérience de stratégie d'enregistrement, dans laquelle vous pouvez également modifier la fréquence d'enregistrement pour des types de ressources spécifiques ou exclure des types de ressources spécifiques de l'enregistrement. Cela peut vous aider à adapter vos paramètres à vos exigences granulaires.	26 novembre 2023

Les types de données suivants sont ajoutés :

- RecordingMode
- RecordingModeRemplacer

Les types de données suivants sont mis à jour :

- PutConfigurationEnregistreur
- ConfigurationRecorder
- BaseConfigurationArticle
- ConfigurationItem

Les pages suivantes du guide du développeur sont mises à jour :

- Ressources de recodage AWS
- Configuration à l' AWS Config aide de la AWS Config console | Configuration en un clic
- Configuration à l' AWS Config aide de la AWS Config console | Configuration manuelle
- Configuration à l' AWS Config aide de la AWS CLI

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, AWS Mainframe Modernization Amazon MemoryDB pour Redis, Amazon, Amazon, Amazon AWS Organizations Relational Database Service (QuickSightAmazon RDS), Amazon Redshift, Amazon Route 53, et. AWS Service Catalog AWS Transfer Family Les politiques `AWSConfigServiceRolePolicy` et `AWS_ConfigRole` ajoutent également désormais des identifiants de sécurité (SID) pour `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` , et la politique `AWSConfigServiceRolePolicy` .	17 novembre 2023

	Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • acm-pca-root-ca-disabled • dynamodb-table-deletion-protection-enabled • ec2-client-vpn-connection-log-enabled • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-configured • fsx-openzfs-copy-tags-enabled • fsx-lustre-copy-tags-to-backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-enabled • neptune-cluster-multi-az-enabled • opensearch-update-check • s3-access-point-in-vpc-only • s3-access-point-public-access-blocks • s3-bucket-mfa-delete-enabled	9 novembre 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les AWS Config modifications de configuration apportées aux nouveaux AWS Identity and Access Managemen t (IAM), AWS Private Certificate Authority (AWS Private CA) AWS Network Manager, Amazon Connect AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS),,, Amazon Managed Streaming AWS IoT TwinMaker pour Apache Kafka Connect (Amazon MSK Connect) et aux ressources types. AWS IoT AWS Lambda Explorateur de ressources AWS Pour plus d'informations, consultez Types de ressource s pris en charge.	3 novembre 2023
AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour le pack de conformité suivant : Meilleures pratiques opérationnelles pour BNM RMiT	26 octobre 2023

Tableaux de bord de conformité et d'inventaire pour les agrégateurs	Avec cette version, AWS Config ajoute une page de tableau de bord de conformité et une page de tableau de bord d'inventaire à la vue agrégée dans la AWS Config console. Sur la page du tableau de bord d'inventaire, vous pouvez consulter les tableaux de bord automatisés avec des widgets qui résument les informations sur la conformité des ressources au sein de votre agrégateur, telles que les 10 principaux types de ressources selon le nombre de ressources non conformes, les 10 principaux packs de conformité au niveau du compte selon le nombre de règles non conformes, etc. Sur la page du tableau de bord d'inventaire, vous pouvez consulter le tableau de bord automatisé avec des widgets qui résument les informations sur les données de configuration des ressources au sein de votre agrégateur, telles que les 10 principaux types de ressources selon le nombre de ressources, les 10 principaux comptes selon le nombre de ressources, etc.	23 octobre 2023

	Pour plus d'informations sur les graphiques et les tableaux, consultez Tableau de bord de conformité et Tableau de bord d'inventaire.	
Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour AWS Private CA, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon Evidently , CloudWatch Amazon Managed Grafana, Amazon, Amazon, GuardDuty Amazon AWS IoT AWS IoT TwinMaker Inspector,,,, Amazon Managed Streaming for Apache Kafka (Amazon AWS Lambda MSK AWS Network Manager),,, et Amazon. AWS Organizations SageMaker Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	4 octobre 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées aux nouveaux types AWS IoT de AWS IoT TwinMaker ressources AWS IoT Wireless Amazon Personalize Amazon Managed Streaming for Apache Kafka (Amazon MSK) SageMaker , Amazon AppStream, AWS CodeBuild Amazon et Amazon Inspector. AWS Config Pour plus d'informations, consultez Types de ressources pris en charge.	4 octobre 2023

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • docdb-cluster-deletion-protection-enabled • docdb-cluster-audit-logging-enabled • docdb-cluster-snapshot-public-prohibited • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-upgrade-check • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-enabled • route53-query-logging-enabled • rds-aurora-mysql-audit-logging-enabled • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled	21 septembre 2023

	• wafv2-rulegroup-logging-enabled • msk-in-cluster-node-require-tls	
AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour Amazon S3 • Bonnes pratiques de fonctionnement pour EC2	8 septembre 2023
Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique supprime désormais les autorisations pour AWS Systems Manager (Systems Manager). Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	6 septembre 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées AWS Config aux nouveaux types de ressources Amazon CodeGuru Profiler, AWS Elemental MediaConnect, AWS Transfer Family, Amazon Managed Service for Prometheus et aux nouveaux types de AWS Batch ressources AWS Cloud Map. Amazon Route 53 Resolver Pour plus d'informations, consultez Types de ressources pris en charge.	6 septembre 2023

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • athena-workgroup-encrypted-at-rest • neptune-cluster-iam-database-authentication • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-export-enabled • neptune-cluster-deletion-protection-enabled • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-check • neptune-cluster-encrypted • neptune-cluster-snapshot-public-prohibited • docdb-cluster-backup-retention-check • docdb-cluster-encrypted • rds-cluster-encrypted-at-rest	10 août 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées aux nouveaux AWS Amplify types Amazon Athena AppIntegrations AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidently, Amazon Forecast CloudWatch , Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS IoT Greengrass Version 2 AWS Ground Station AWS Elemental MediaConvert AWS Elemental MediaTailor, Amazon Personalize, Amazon Pinpoint et les types de ressources. AWS Config AWS Resilience Hub Pour plus d'informations, consultez Types de ressources pris en charge.	3 août 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Managed Workflows pour AWS App Mesh, Amazon AppStream 2.0 AWS CloudFormation, Amazon CloudFront AWS CodeArtifact, Amazon Connect AWS CodeBuild, Amazon AWS Glue, AWS Identity and Access Management (IAM) GuardDuty, Amazon Inspector,,,, AWS IoT AWS IoT TwinMaker AWS IoT Wireless, Amazon Managed Streaming pour Apache Kafka, Amazon Macie AWS Elemental MediaConnect,,,,, AWS Network Manager AWS Organizations, Amazon Route 53 Explorateur de ressources AWS, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) et systèmes Amazon EC2 Directeur (SSM). Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	28 juillet 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les AWS Config modifications de configuration apportées aux nouveaux Amazon Kinesis, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon Connect,, , et () types de ressource s. AWS CloudFormation AWS AppConfig AWS App Mesh AWS App Runner AWS Database Migration Service AWS DMS Pour plus d'informa tions, consultez Types de ressources pris en charge.	10 juillet 2023
Les limites de services augmentent pour les packs de conformité des organisations	Cette version AWS Config prend en charge 350 AWS Config règles par région et par compte dans tous les packs de conformité et 350 AWS Config règles organisationnelles par organisation. Pour plus d'informations, consultez Limites de service .	13 juin 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Managed Workflows pour Amazon Connect AWS Amplify AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena,,,,,, Amazon, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast,,,, (IAM), Amazon Streaming AWS Identity and Access Management géré pour Apache Kafka (Amazon MSK) AWS Organizations, AWS IoT Greengrass AWS Ground Station Amazon Lightsail, Amazon Logs, CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon QuickSight, AWS Migration Hub Refactor Spaces Amazon Simple	13 juin 2023

Storage Service (Amazon S3), Amazon, et. SageMaker AWS Transfer Family Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.

AWS Config Exclusions d'enregistrement par type de ressource	Cette version vous AWS Config permet d'exclure des types spécifiques de AWS ressources du suivi des stocks et de la surveillance de la conformité tout en continuant à suivre tous les autres types de ressources pris en charge actuellement disponibles dans AWS Config, y compris ceux qui seront ajoutés à l'avenir. Vous pouvez utiliser cette fonctionnalité pour cibler les ressources critiques soumises à vos normes de conformité et de gouvernance. Les mises à jour de l'API pour l'enregistreur de configuration et le groupe d'enregistrement sont rétrocompatibles, ce qui signifie qu'elles fonctionnent avec les versions précédentes de l'API PutConfigurationRecorder. Vous pouvez continuer à gérer les types de ressources enregistrés exactement de la même manière qu'auparavant, sans utiliser de nouvelles API ou celles qui ont été mises à jour. Les types de données suivants sont ajoutés : • RecordingStrategy • ExclusionByResourceTypes	9 juin 2023

Les types de données suivants sont mis à jour :

- PutConfigurationEnregistreur
- ConfigurationRecorder
- RecordingGroup

La page suivante du guide du développeur est mise à jour :

- Sélection des ressources qui sont enregistrées

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées aux nouveaux Amazon Elastic Container Service (Amazon ECS), Amazon Keyspaces (pour Apache Cassandra) (Amazon Keyspaces),,,,,, Amazon AppStream 2.0 AWS Signer AWS Amplify AWS App Mesh, AWS App Runner Amazon Elastic Compute Cloud (Amazon EC2) AWS CodeArtifact, Amazon CloudWatch Evidently, Amazon Forecast (AWS Identity and Access Management IAM), Types de ressources Amazon Pinpoint, Amazon, Amazon Data Firehose. AWS Config SageMaker AWS Transfer Family Pour plus d'informations, consultez Types de ressources pris en charge.	5 juin 2023

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • cloudfront-s3-origin-access-control-enabled • custom-schema-registry-policy-attached • ec2-client-vpn-not-authorize-all • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade-enabled • mq-cloudwatch-audit-logging-enabled • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-enabled	10 mai 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les AWS Config modifications de configuration apportées aux nouveaux Amazon Route 53 Resolver types de ressource s Amazon Elastic Compute Cloud (Amazon EC2) AWS IoT , Wireless,, AWS Network Manager, AWS Device Farm, Amazon AWS Ground Station, AppFlow Amazon Redshift, Amazon Pinpoint,,, EC2 Image Builder AWS IoT AWS AppConfig, Amazon Runtime SageMaker , AWS Panorama Amazon ECR et autres types de ressources. CloudWatc h AWS Audit Manager Pour plus d'informations, consultez Types de ressources pris en charge.	5 mai 2023
AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configura tion apportées à`AWS::Netw orkFirewall::TLSIn spectionConfigurat ion` . Pour plus d'informa tions, consultez Types de ressources pris en charge.	1er mai 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Managed Workflows pour AWS Amplify AWS App Mesh AWS App Runner,, Amazon CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon, SageMaker AWS Transfer Family Amazon Pinpoint, Resilience Hub, Amazon AWS Migration Hub AWS , AWS Directory Service CloudWatch, et. AWS WAF Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	13 avril 2023

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-enabled • elasticache-repl-grp-encrypted-at-rest • elasticache-repl-grp-encrypted-in-transit • elasticache-repl-grp-redis-auth-enabled • elasticache-subnet-group-check • cloudfront-s3-origin-non-existent-bucket	10 avril 2023
Les limites de services augmentent pour les packs de conformité des organisations	Cette version AWS Config prend en charge 350 AWS Config règles par compte dans tous les packs de conformité de l'organisation. Pour plus d'informations, consultez Limites de service .	3 avril 2023

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-rest	3 avril 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées aux nouveaux flux Amazon AppStream 2.0, AWS Auto Scaling, Amazon Connect, Amazon Elastic Compute Cloud EventBridge, Amazon HealthLake, Kinesis Video Stream, Lookout for Vision AWS IoT TwinMaker, Network Manager, Amazon Pinpoint, Amazon Route 53 Application Recovery Controller et aux types de ressources. AWS Config AWS RoboMaker Pour plus d'informations, consultez Types de ressources pris en charge.	3 avril 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Managed Workflows for Amazon AppFlow AWS App Runner, Amazon AppStream 2.0, Amazon AWS CloudFormation, CloudFront,,, CloudWatch AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidently, CloudWatch Amazon Forecast, (AWS IoT IAM), AWS Ground Station Amazon AWS Identity and Access Management MemoryDB for Redis, Amazon Pinpoint AWS Network Manager, AWS Panorama Amazon Relational Database Service Service (Amazon RDS), Amazon Redshift et Amazon. SageMaker Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	30 mars 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour AWS Audit Manager. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	3 mars 2023
AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les AWS Config modifications de configuration apportées aux nouveaux types de ressources AWS Elemental MediaPackage, Amazon EventBridge AWS IoT,, (Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Lookout for Metrics, Amazon Lex AWS Device Farm, CodeGuru , Amazon Reviewer et AWS Budgets autres types de ressources. Amazon Route 53 Resolver AWS RoboMaker Pour plus d'informations, consultez Types de ressources pris en charge.	2 mars 2023

Mise à jour de sécurité IAM	AWS Config suit désormais les modifications apportées à la `AWSConfigMultiAccountSetupPolicy` politique. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	27 février 2023
AWS Config Couverture des ressources par région : disponibilité	Cette version AWS Config fournit des informations régionales pour chaque type de ressource pris en charge. Pour en savoir plus sur les types de ressources pris en charge selon les régions, consultez Couverture des ressources en fonction de la disponibilité dans les régions.	20 février 2023

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées aux nouveaux Amazon Interactive Video Service (Amazon IVS), Amazon Simple Storage Service (Amazon AWS Glue S3), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon AWS IoT Relational Database Service (Amazon RDS) et Managed Service for Apache Types de ressources de lien. AWS Config Pour plus d'informations, consultez Types de ressources pris en charge.	7 février 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Managed Workflows pour Apache Airflow AWS IoT, Amazon AppStream 2.0, Amazon CodeGuru Reviewer AWS HealthLake, Amazon Kinesis Video Streams, Amazon Route 53 Application Recovery Controller AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon AWS Identity and Access Management Pinpoint (IAM), Amazon et Amazon Logs. GuardDuty CloudWatch Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	1er février 2023
Mise à jour de sécurité IAM	À titre de bonne pratique de sécurité, la politique `ConfigConformsServiceRolePolicy` supprime désormais les autorisations étendues au niveau des ressources pour `config:DescribeConfigRules` . Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	12 janvier 2023

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires à Amazon Managed Service pour Prometheus AWS Audit Manager,,,,AWS DMS() AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud (Amazon EC2 AWS Glue) AWS IoT,, Amazon Lightsail AWS Elemental MediaPackage,,, Amazon, Amazon Route 53 Application Recovery Controller AWS Network Manager QuickSight, AWS Resource Access Manager Amazon Simple Storage Service (Amazon S3) et Amazon Timestream Timestream. AWS Directory Service Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	10 janvier 2023

AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications de configuration apportées aux nouveaux EventBrid ge schémas Amazon MQ, AWS Cloud9 Amazon AWS AppConfig, Amazon Fraud Detector, Amazon AWS IoT Analytics Lightsail AWS Elemental MediaPackage (MediaPackage) AWS IoT, Amazon Route 53 Applicati on Recovery Controller et aux types de ressources. AWS Config AWS Resilience Hub AWS Transfer Family Pour plus d'informations, consultez Types de ressources pris en charge.	5 janvier 2023
AWS Config règle la couvertur e des ressources	Dans cette version, AWS Config affiche la couverture des types de ressources pour un nombre accru de règles AWS Config gérées.	21 décembre 2022
AWS Config découvrabilité des règles	Cette version AWS Config prend en charge les pages de liste des règles AWS Config gérées par mode d'évaluat ion, de liste des règles AWS Config gérées par type de déclencheur et de liste des règles AWS Config gérées par disponibilité par région.	21 décembre 2022

AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour K-ISMS • Bonnes pratiques de fonctionnement pour NIST 800 171 • Bonnes pratiques de fonctionnement pour PCI DSS 3.2.1 • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau élevé) • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau modéré) • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau faible) • Bonnes pratiques de fonctionnement pour NZISM • Bonnes pratiques de fonctionnement pour NIST 800-53 rev 5	19 décembre 2022

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-disabled • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-access-check • security-account-information-provided • storagegateway-resources-protected-by-backup-plan • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	9 décembre 2022

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez enregistrer AWS Config les modifications de configuration apportées aux nouveaux types de ressource s Amazon CloudWatch RUM EventBridge GuardDuty, Amazon, Amazon, Amazon Simple Email Service (Amazon SES) AWS Backup AWS DataSync,, AWS Fault Injection Service et AWS FIS(). Pour plus d'informations, consultez Types de ressource s pris en charge.	9 décembre 2022

AWS Config Conformité proactive	Cette version AWS Config permet de vérifier de manière proactive la conformité aux AWS Config règles avant le provisionnement des ressources. Elle vous permet d'évaluer les paramètres de configuration de vos ressource s avant leur création ou leur mise à jour. Utilisez-le AWS Config pour suivre les modifications de configuration apportées à vos ressource s, que ce soit avant ou après le provisionnement, et pour vérifier si vos ressources correspondent aux configura tions souhaitées. Les types de données suivants sont ajoutés : • GetResourceEvaluat ionSummary • StartResourceÉvaluation • ListResourceÉvaluations Les types de données suivants sont mis à jour : • DescribeConfigRulesFilters • GetComplianceDetai lsByRessource • EvaluationResultQualificate ur	28 novembre 2022

- EvaluationModeConfiguration

Les pages suivantes du guide du développeur sont mises à jour :

- Composantes d'une AWS Config règle
- Mode d'évaluation et types de déclencheurs pour les AWS Config règles
- AWS Config Règles gérées
- AWS Config Règles personnalisées
- Gérer vos AWS Config règles

Détection de dérive en tant qu'élément de configuration (CI) pour l'enregistreur AWS Config de configuration	Dans cette version, AWS Config suit toutes les modifications apportées à l'enregistreur de configuration pour indiquer si l'état de l'enregistreur de configuration est différent ou s'il a dérivé de son état précédent ; par exemple, si des mises à jour ont été apportées aux types de ressources que vous avez activé AWS Config pour le suivi, si vous avez arrêté ou démarré l'enregistreur de configuration, ou si vous avez supprimé ou désinstallé l'enregistreur de configuration. Le type de `AWS::Config::ConfigurationRecorder` ressource est un type de ressource système AWS Config et l'enregistrement de ce type de ressource est activé par défaut dans toutes les régions prises en charge. L'enregistrement du type de ressource `AWS::Config::ConfigurationRecorder` est effectué sans frais supplémentaires. Pour plus d'informations, consultez Détection des dérives pour l'enregistreur de configuration.	18 novembre 2022

AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications de configuration apportées aux nouveaux types de AWS IoT Events ressources AWS Cloud Map EC2 Image Builder AWS DataSync,, AWS Glue, Amazon Route 53 Applicati on Recovery Controller et Amazon Elastic Container Registry (Amazon ECR). AWS Config Pour plus d'informa tions, consultez Types de ressources pris en charge.	8 novembre 2022
Mise à jour de sécurité IAM	La `AWSConfigServiceRo lePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour AWS CloudFormation. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	7 novembre 2022

AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour la division Criminal Justice Information Services (CJIS) • Bonnes pratiques en matière de sécurité pour Amazon SageMaker • Bonnes pratiques de sécurité pour Amazon Elastic Container Registry Les packs de conformité suivants sont mis à jour : • Bonnes pratiques de fonctionnement pour MAS TRMG • Bonnes pratiques de fonctionnement pour NCSC Cyber Assesment Framework • Bonnes pratiques de fonctionnement pour les principes de sécurité du cloud NCSC	27 octobre 2022

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour AWS Certificate Manager Amazon Managed Workflows for Apache Airflow AWS Amplify, Amazon Keyspaces AWS AppConfig, Amazon, Amazon Connect, CloudWatch Amazon Elastic Compute Cloud (Amazon EC2) AWS Glue DataBrew, Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Fraud Detector, Amazon FSx EventBridge, AWS Fault Injection Service Amazon Amazon, Amazon GameLift Location Service, Amazon AWS IoT Lex, Amazon Lightsail, Amazon Pinpoint,,,, Amazon, Amazon Relational AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Database Service (Amazon RDS), Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage Service (Amazon S3), et. AWS Cloud Map AWS Security Token Service Pour plus d'informations, consultez	19 octobre 2022

	Politiques gérées par AWS pour AWS Config.	
AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications de configuration apportées aux nouveaux types de ressource s Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Email Service (Amazon AWS AppConfig SES) AWS Cloud Map et aux nouveaux types de ressources. AWS Config AWS DataSync Pour plus d'informations, consultez Types de ressources pris en charge.	6 octobre 2022
AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configura tion apportées aux nouveaux types Amazon GuardDuty SageMaker, Amazon AWS AppSync AWS Cloud Map,, et de AWS DataSync ressource s. Pour plus d'informations, consultez Types de ressource s pris en charge.	4 octobre 2022
AWS Config prend en charge le nouveau pack de conformité	Avec cette version, AWS Config met à jour les meilleure s pratiques opérationnelles pour le pack de conformité SWIFT CSP.	4 octobre 2022

AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 1 • Bonnes pratiques de fonctionnement pour CMMC 2.0 niveau 2 Les packs de conformité suivants sont mis à jour : • Bonnes pratiques de fonctionnement pour Amazon API Gateway • Meilleures pratiques opérationnelles pour le pilier de fiabilité du AWS framework Well-Architected • Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected • Bonnes pratiques de fonctionnement pour CMMC niveau 1 • Bonnes pratiques de fonctionnement pour CMMC niveau 2 • Bonnes pratiques de fonctionnement pour CMMC niveau 3	30 septembre 2022

	• Bonnes pratiques de fonctionnement pour CMMC niveau 4 • Bonnes pratiques de fonctionnement pour CMMC niveau 5 • Bonnes pratiques de fonctionnement pour FFIEC • Bonnes pratiques de fonctionnement pour FedRAMP(Low) • Bonnes pratiques de fonctionnement pour MAS Notice 655 • Bonnes pratiques de fonctionnement pour NBC TRMG • Bonnes pratiques de fonctionnement pour NIST 800 172	
Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour AWS Glue. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	14 septembre 2022
AWS Config prend en charge le nouveau pack de conformité	Cette version AWS Config prend en charge les meilleures pratiques opérationnelles pour le pack de conformité SWIFT CSP.	9 septembre 2022

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires à Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR EventBridge, Amazon, Amazon, Amazon Fraud Schemas, Amazon Detector, EventBridge Amazon Amazon FinSpace, Amazon Interactive Video Service (Amazon IVS), Amazon Managed Service pour Apache Flink, EC2 Image GameLift Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble QuickSight Pinpoint, Amazon, StudioAmazon Amazon Route 53 Application Recovery Controlle	7 septembre 2022

r, Amazon Simple Storage Service (Amazon S3) Amazon Route 53 Resolver Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,, ,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events, AWS IoT SiteWise, AWS IoT TwinMaker, AWS Lake Formation AWS License Manager, AWS Resilience Hub, AWS Signer, et AWS Transfer Family. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.

AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques opérationnelles pour Amazon CloudWatch • Bonnes pratiques de fonctionnement Germany Cloud Computing Compliance Controls Catalog (C5) • Bonnes pratiques de fonctionnement pour IRS 1075 Les packs de conformité suivants sont mis à jour : • AWS Pack de conformité aux rambardes Control Tower Detective • Bonnes pratiques de fonctionnement pour CISA Cyber Essentials • Bonnes pratiques de fonctionnement pour le guide de la cybersécurité pour les PME de l'ENISA • Bonnes pratiques de fonctionnement pour le titre 21 CFR Part 11 de la FDA • Bonnes pratiques de fonctionnement pour FedRAMP (modéré)	31 août 2022

	• Bonnes pratiques de fonctionnement pour la sécurité HIPAA • Bonnes pratiques de fonctionnement pour le cadre de confidentialité NIST v1.0 • Bonnes pratiques de fonctionnement pour NYDFS 23 • Bonnes pratiques de fonctionnement pour le cadre de cybersécurité RBI pour les UCB • Bonnes pratiques de fonctionnement pour RBI MD-ITF	
Mise en route AWS Config et mises à jour du pack de conformité personnalisé	Cette version AWS Config met à jour les pages Getting Started with the Console AWS Config et Setup up AWS Config with the Console, en introduisant une page de configuration en un clic et une page de configuration manuelle. AWS Config met également à jour la page du pack de conformité personnalisé avec une procédure pas à pas expliquant comment créer un fichier YAML de pack de conformité à partir de zéro.	25 août 2022

AWS Systems Manager Intégration du document (document SSM) aux packs de conformité	Cette version vous permet de créer un modèle de pack de conformité à l'aide d'un document SSM. Pour plus d'informations sur les documents SSM, consultez Documents AWS Systems Manager dans le Guide de l'utilisateur AWS Systems Manager . Les types de données suivants sont mis à jour : • PutConformancePack • ConformancePackDétail • Modèles SM DocumentDetails Les pages suivantes du guide du développeur sont mises à jour : • Déploiement d'un pack de conformité à l'aide de la console AWS Config • Déploiement d'un pack de conformité à l'aide de l'interface de ligne de AWS commande	24 août 2022

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Simple Email Service (Amazon SES) AWS DataSync, AWS Cloud Map et. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	22 août 2022
AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les AWS Config modifications de configuration apportées aux nouveaux types de ressources Amazon Athena, Amazon Detective, SageMaker Amazon, AWS Database Migration Service Amazon Route 53 AWS Glue, AWS Key Management Service (AWS KMS), () et Amazon Simple Email Service (Amazon SES).AWS DMS Pour plus d'informations, consultez Types de ressources pris en charge.	16 août 2022

AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour NIST 1800 25 • Bonnes pratiques de fonctionnement pour NIST 800 181 • Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Standard • Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Material • Bonnes pratiques de fonctionnement pour ACSC Essentials 8 • Bonnes pratiques de fonctionnement pour ACSC ISM • Bonnes pratiques de fonctionnement pour APRA CPG 234 • Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 1 • Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 2	1er août 2022

- Bonnes pratiques de fonctionnement pour BNM RMiT
- Bonnes pratiques de fonctionnement pour NIST CSF

Score de conformité des packs de conformité	Cette version AWS Config introduit le score de conformité pour les packs de conformité, qui vous fournit une vue globale de l'état de conformité de vos packs de conformité. Vous pouvez l'utiliser pour identifier, étudier et déterminer le niveau de conformité de vos packs de conformité. Le score de conformité est le pourcentage du nombre de combinaisons règle-ressource conformes dans un pack de conformité par rapport au nombre total de combinaisons règles-ressources possibles dans le pack de conformité. Les types de données suivants sont mis à jour : • ListConformancePackComplianceScores • ConformancePackComplianceScore Les pages suivantes du guide du développeur sont mises à jour : • Afficher le AWS Config tableau de bord • Affichage des données de conformité dans le tableau	26 juillet 2022

	de bord des packs de conformité • Gestion des packs de conformité (API)	
Mise à jour de sécurité IAM	La `ConfigConformsServiceRolePolicy` politique autorise désormais la publication de points de données métriques sur Amazon CloudWatch. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	25 juillet 2022

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires à Amazon Elastic Container Service (Amazon ECS), Amazon, Amazon ElastiCache, Amazon FSx EventBridge, Amazon Managed Service pour Apache Flink, Amazon Location Service, Amazon Managed Streaming pour Apache Kafka, Amazon Rekognition, QuickSight Amazon Simple Storage (Amazon S3) Simple Storage S3), Amazon Simple Email Service (Amazon SES),,,,, ,,, (IAM Identity Center) AWS Amplify, EC2 Image Builder AWS DataSync, AWS RoboMaker AWS AppConfig AWS AppSync AWS Billing Conductor AWS Firewall Manager AWS Glue AWS IAM Identity Center et Elastic Load Balancing. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	15 juillet 2022

AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications AWS Config de configuration apportées aux nouveaux types de ressources Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez Types de ressources pris en charge.	8 juillet 2022
AWS Config prend en charge un nouveau type de ressources	Avec cette version, vous pouvez AWS Config enregistrer les modifications de configuration apportées aux nouveaux types de AWS Global Accelerator ressources. Pour plus d'informations, consultez Types de ressources pris en charge.	5 juillet 2022
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • autoscaling-launch-template • ecs-task-definition-log-configuration • ecs-awsvpc-networking-enabled • nlb-cross-zone-load-balancing-enabled	1et juillet 2022

AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour le profil moyen de contrôle du cloud du Canadian Centre for Cyber Security (CCCS) • Bonnes pratiques de fonctionnement pour Gramm Leach Bliley Act (GLBA) • Bonnes pratiques de fonctionnement pour GxP EU Annex 11 • Bonnes pratiques de sécurité pour Amazon Elastic Kubernetes Service (Amazon EKS) • Bonnes pratiques de sécurité pour Amazon Relational Database Service (Amazon RDS) • Bonnes pratiques de sécurité pour AWS Lambda Les packs de conformité suivants sont mis à jour : • Bonnes pratiques de fonctionnement pour l'IA et le ML • Bonnes pratiques de fonctionnement pour Amazon DynamoDB	30 juin 2022

	• Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG1 • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG2 • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG3 • Bonnes pratiques de fonctionnement pour la sécurité HIPAA • Bonnes pratiques de fonctionnement pour NIST 800-53 rev 5 • Bonnes pratiques de fonctionnement pour NIST CSF	
AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées aux nouveaux types de SageMaker ressources Amazon. Pour plus d'informations, consultez Types de ressources pris en charge.	29 juin 2022

AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications de configuration apportées aux nouveaux types de ressources Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Route 53, Amazon WorkSpace s AWS Batch, AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), AWS Database Migration Service (AWS DMS) et Elastic AWS Step Functions Load Balancing. AWS Config Pour plus d'informations, consultez Types de ressource s pris en charge.	14 juin 2022

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • aurora-last-backup-recovery-point-created • dynamodb-last-backup-recovery-point-created • ebs-last-backup-recovery-point-created • ec2-last-backup-recovery-point-created • efs-last-backup-recovery-point-created • fsx-last-backup-recovery-point-created • rds-last-backup-recovery-point-created • s3-last-backup-recovery-point-created • storagegateway-last-backup-recovery-point-created • virtualmachine-last-backup-recovery-point-created	13 juin 2022

AWS Config Intégration avec AWS Security Hub	Dans cette version, vous pouvez consulter les résultats des évaluations de règles AWS Config gérées et personnalisées sous forme de conclusions dans AWS Security Hub. Security Hub transforme les évaluations des règles en résultats, qui fournissent plus d'informa tions sur les ressource s concernées, telles que l'Amazon Resource Name (ARN) et la date de création. Ces résultats peuvent être consultés en même temps que d'autres résultats de Security Hub, en fournissant une vue d'ensemble complète de votre niveau de sécurité. Pour plus d'informations, consultez Envoi des évaluations de règles à Security Hub	7 juin 2022

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour Amazon Athena, Amazon Detective GuardDuty, Amazon, Amazon Macie, Amazon Simple Email Service (Amazon AWS Glue SES) AWS Resource Access Manager ,AWS RAM() et. AWS IAM Identity Center Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	31 mai 2022

AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de sécurité pour Amazon Elastic Container Service (Amazon ECS) • Bonnes pratiques de sécurité pour Amazon Elastic File System (Amazon EFS) • Bonnes pratiques en matière de sécurité pour Amazon CloudFront • Bonnes pratiques de sécurité pour AWS Auto Scaling • Bonnes pratiques de sécurité pour AWS Network Firewall • Bonnes pratiques de sécurité pour AWS Secrets Manager	31 mai 2022

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées aux nouveaux types d'Amazon SageMaker et de AWS Step Functions ressources. Pour plus d'informations, consultez Types de ressources pris en charge.	26 mai 2022
AWS Config prend en charge le nouveau pack de conformité	Avec cette version, AWS Config met à jour les meilleures pratiques opérationnelles pour le pack de conformité NERC CIP BCSI.	20 mai 2022
Composantes d'une AWS Config règle	Dans cette version, AWS Config introduit une page Composants d'une AWS Config règle. La page décrit la structure des définitions de règles, les métadonnées des règles et les meilleures pratiques pour écrire des règles avec Python à l'aide du kit de développement de AWS Config règles (RDK) et de la bibliothèque de kits de développement de AWS Config règles (RDKlib).	9 mai 2022

Les limites de services augmentent pour les packs de conformité des organisations	Cette version AWS Config prend en charge 180 AWS Config règles par compte dans tous les packs de conformit é de l'organisation. Pour plus d'informations, consultez Limites de service .	6 mai 2022
AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de sécurité pour Amazon OpenSearch Service • Bonnes pratiques de sécurité pour Amazon Redshift • Bonnes pratiques de sécurité pour AWS CloudTrail • Bonnes pratiques de sécurité pour AWS CodeBuild • Bonnes pratiques de sécurité pour AWS WAF	29 avril 2022
AWS Config met à jour la règle gérée	Dans cette version, AWS Config prend en charge la règle gérée s3-resources-protected-by-backup-plan.	11 avril 2022

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais des autorisations supplémentaires pour obtenir des informations sur tout ou un magasin de données d' AWS CloudTrail événements (EDS) spécifique ou spécifique, obtenir des informations sur toutes les ressources ou sur une AWS CloudFormation ressource spécifiée, obtenir la liste d'un groupe de paramètres ou d'un groupe de sous-réseaux de l'accélérateur DynamoDB (DAX), obtenir des informations AWS Database Migration Service sur AWS DMS() les tâches de réplication pour votre compte dans la région actuellement consultée et obtenir une liste de toutes les politiques d'un type spécifié. AWS Organizations Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	7 avril 2022

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-limit • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-version • netfw-policy-default-action-fragment-packets • netfw-policy-default-action-full-packets • netfw-policy-rule-group-associated • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-empty • waf-regional-rulegroup-not-empty • waf-regional-webacl-not-empty	4 avril 2022

- vpc-peering-dns-resolution-check

AWS Config Règles de politique personnalisées	Avec cette version, vous AWS Config pouvez créer des règles de politique AWS Config personnalisées à l'aide de AWS CloudFormation Guard (guard). Guard est un policy-as-code langage qui vous permet d'écrire des politiques qui sont appliquées AWS Config sans avoir à créer de fonctions Lambda pour gérer vos règles personnal isées. Les règles rédigées à l'aide de la politique Guard peuvent être créées à partir de la AWS Config console ou à l'aide des API de AWS Config règles. Les pages suivantes du guide du développeur sont mises à jour : • Règles AWS Config pe rsonnalisées • Création de règles AWS Config personnalisées avec Guard Les types de données suivants sont mis à jour : • Source • CustomPolicyDétails • ConfigRuleEvaluationStatus • GetCustomRulePolicy	4 avril 2022

	• GetOrganizationCustomRulePolitique • OrganizationCustomPolicyRuleMétadonnées	
AWS Config prend en charge un nouveau type de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au nouveau type de SecurityConfiguration ressource Amazon EMR. Pour plus d'informations, consultez Types de ressources pris en charge.	31 mars 2022
AWS Config met à jour la règle gérée	Avec cette version, AWS Config prend en charge la règle gérée virtualmachine-resources-protected-by-backup-plan.	29 mars 2022

AWS Config Intégration avec Amazon CloudWatch Metrics	Cette version prend AWS Config désormais en charge le suivi de votre AWS Config utilisation et de vos indicateurs de réussite avec Amazon sur CloudWatch la page du AWS Config tableau de bord. CloudWatch metrics est un service de surveillance qui fournit des données sur les performances de vos systèmes, notamment la possibilité de rechercher, de représenter graphiquement et de créer des alarmes sur la base de mesures relatives AWS aux ressources. À partir du AWS Config tableau de bord, vous pouvez voir quel trafic est à l'origine de votre AWS Config consommation et connaître les indicateurs clés des défaillances survenues dans votre flux de travail. La page suivante est mise à jour : • Afficher le AWS Config tableau de bord	29 mars 2022

AWS Config prend en charge un nouveau type de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au nouveau type de ressource Amazon GuardDuty Detector. Pour plus d'informations, consultez Types de ressources pris en charge.	24 mars 2022

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • clb-multiple-az • cloudfront-no-deprecated-ssl-protocols • cloudfront-traffic-to-origin-encrypted • cloudwatch-alarm-action-enabled-check • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-attach-disabled • ecr-private-lifecycle-policy-configured • efs-access-point-enforce-root-directory • efs-access-point-enforce-user-identity • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-check • s3-event-notifications-enabled • sns-topic-message-delivery-notification-enabled • waf-global-rulegroup-not-empty	23 mars 2022

- waf-global-rule-not-empty

AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG1 • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG2 • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG3 • Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau faible) • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau modéré) • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau élevé) • Bonnes pratiques de fonctionnement pour MAS Notice 655 • Bonnes pratiques de fonctionnement pour NIST 1800-25	16 mars 2022

Mise à jour de sécurité IAM	Les politiques `AWSConfigServiceRolePolicy` et `AWS_ConfigRole` accordent désormais des autorisations supplémentaires pour AWS CloudFormation. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	14 mars 2022
AWS Config met à jour les règles gérées	Avec cette version, AWS Config met à jour les règles gérées suivantes : • aurora-resources-protected-by-backup-plan • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	10 mars 2022

AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications de configuration apportées AWS Config aux nouveaux types de ressources publiques d'Amazon Elastic Container Registry. Pour plus d'informations, consultez Types de ressources pris en charge.	4 mars 2022
AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications AWS Config de configuration apportées aux nouveaux types de ressources Amazon Elastic Compute Cloud. Pour plus d'informations, consultez Types de ressources pris en charge.	28 février 2022
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • codedeploy-auto-rollback-monitor-enabled • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-disabled	25 février 2022

Journalisation et surveillance en cours de AWS Config mise à jour	Avec cette version, AWS Config met à jour la page Monitoring AWS Config with Amazon EventBridge Events afin de remplacer les références à Amazon CloudWatch Events. Amazon EventBridge est le moyen préféré pour gérer vos événements. CloudWatch Les événements et la même API EventBridge constituent le même service sous-jacent et la même API, mais EventBridge offrent davantage de fonctionnalités. Les modifications que vous apportez dans l'une CloudWatch ou l'autre des consoles ou EventBridge apparaîtront dans chaque console. Pour plus d'informations, consultez Amazon EventBridge.	24 février 2022

AWS Page SDK pour AWS Config	Dans cette version, AWS Config introduit une page d'utilisation AWS Config avec un AWS SDK. AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque SDK fournit une API, des exemples de code et de la documentation qui faciliten t la création d'applications par les développeurs dans leur langage préféré.	24 février 2022

Mise à jour de la politique d'approbation de la sécurité du rôle IAM	Avec cette version, AWS Config met à jour la déclaration de politique de confiance IAM afin d'inclure des protections de sécurité dans la politique de confiance qui limitent l'accès avec `sourceARN` et/ou `sourceAccountId` pour l'opération AWS Security Token Service (AWS STS). Elle garantit ainsi que la politique d'approbation du rôle IAM accède à vos ressources uniquement pour le compte des utilisateurs et des scénarios attendus. La page suivante est mise à jour : • Ajout d'une politique d'approbation IAM à votre rôle	18 février 2022

Modifications apportées à l'enregistrement des types de ressources globales	AWS Config modifie désormais la façon dont les nouveaux types de ressource s globales sont enregistrés dans AWS Config Recording . Les types de ressource s globaux sont AWS des ressources pour lesquelle s il n'est pas nécessaire de spécifier une région lors de leur création. Avant cette modification, vous pouviez activer l'enregistrement des types de ressources globales dans toutes les régions prises en charge dans AWS Config. Après cette modificat ion, les nouveaux types de ressources globales intégrés à AWS Config l'enregis trement ne peuvent être enregistrés que dans la région d'origine du service pour la partition commerciale et AWS GovCloud (ouest des États-Unis) pour la partition . AWS GovCloud (US) Vous pourrez désormais consulter les éléments de configura tion de ces nouveaux types de ressources globales uniquement dans leur région d'origine et AWS GovCloud (ouest des États-Unis). Pour obtenir la liste des régions d'origine des types de	18 février 2022

ressources globales intégrés après février 2022, consultez le tableau de la page Enregistrement de tous les types de ressources pris en charge.

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique autorisent désormais à obtenir des informations sur les environnements Elastic Beanstalk et une description des paramètres du jeu de configuration Elastic Beanstalk spécifié, à obtenir une carte des versions d'Elasticsearch, à décrire les groupes d'options Amazon RDS disponibles pour une base OpenSearch de données et à obtenir des informations sur une configuration de déploiement. CodeDeploy Cette politique autorise également désormais à récupérer le contact alternatif spécifié attaché à une Compte AWS, à récupérer des informations sur une politique, à récupérer une AWS Organizations politique de référentiel Amazon ECR, à récupérer des informations sur une AWS Config règle archivée, à récupérer une liste des familles de définitions de tâches Amazon ECS, à répertorier les unités organisationnelles (UO) racine ou parent de l'unité d'organisation ou du compte enfant spécifié, et à répertorier les politique	10 février 2022

s associées à la racine, à l'unité organisationnelle ou au compte cible spécifié. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-check • codebuild-project-logging-enabled • codebuild-project-s3-logs-encrypted • ec2-security-group-attached-to-eni-periodic • ecr-private-image-scanning-enabled • ecr-private-tag-immutability-enabled • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hard-limit • ecs-task-definition-nonroot-user • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-version	10 février 2022

	• eks-cluster-supported-version • lambda-vpc-multi-az-check • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-not-empty • rds-cluster-default-admin-check • rds-db-security-group-not-allowed • rds-instance-default-admin-check • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-empty	
Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais l'autorisation de créer des groupes de CloudWatch journaux et des flux Amazon et d'écrire des journaux dans les flux de journaux créés. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	2 février 2022

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-tolerance • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-encryption-check	31 janvier 2022
AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées aux types de AWS CodeDeploy ressources. Pour plus d'informations, consultez Types de ressources pris en charge.	5 janvier 2022

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées aux nouveaux types de SageMaker ressources Amazon. Pour plus d'informa tions, consultez Types de ressources pris en charge.	20 décembre 2021
AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour le guide de la cybersécurité pour les PME de l'ENISA	20 décembre 2021
AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour NIST 800 172 • Bonnes pratiques de fonctionnement pour NIST 800 181 Le pack de conformité suivant est mis à jour : • Bonnes pratiques de fonctionnement pour K-ISMS	18 novembre 2021

AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour Amazon API Gateway • Bonnes pratiques opérationnelles pour AWS Backup • Bonnes pratiques de fonctionnement pour CISA Cyber Essentials • Bonnes pratiques opérationnelles pour DevOps • Bonnes pratiques de fonctionnement pour le cadre de confidentialité NIST v1.0 Les packs de conformité suivants sont mis à jour : • Bonnes pratiques de fonctionnement pour FedRAMP(Low) • Bonnes pratiques de fonctionnement pour FedRAMP (modéré)	29 octobre 2021

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées aux nouveaux types OpenSearch de ressources Amazon Service. Pour plus d'informations, consultez Types de ressources pris en charge.	12 octobre 2021
AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour le pack de conformité suivant : • Bonnes pratiques de fonctionnement pour MAS TRMG	12 octobre 2021

AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Material • Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Standard • Bonnes pratiques de fonctionnement pour ACSC Essentials 8 • Bonnes pratiques de fonctionnement pour ACSC ISM • Bonnes pratiques de fonctionnement pour BNM RMiT • Bonnes pratiques de fonctionnement pour CMMC niveau 1 • Bonnes pratiques de fonctionnement pour CMMC niveau 2 • Bonnes pratiques de fonctionnement pour CMMC niveau 3 • Bonnes pratiques de fonctionnement pour CMMC niveau 4	30 septembre 2021

- Bonnes pratiques de fonctionnement pour CMMC niveau 5
- Bonnes pratiques de fonctionnement pour le titre 21 CFR Part 11 de la FDA
- Bonnes pratiques de fonctionnement pour FFIEC
- Bonnes pratiques de fonctionnement pour MAS Notice 655
- Bonnes pratiques de fonctionnement pour NBC TRMG
- Bonnes pratiques de fonctionnement pour NERC CIP
- Bonnes pratiques de fonctionnement pour NIST 800-53 rev 5

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais l'autorisation d'obtenir des informations sur un ou plusieurs domaines Amazon OpenSearch Service (OpenSearch Service) et d'obtenir une liste de paramètres détaillée pour un groupe de paramètres de base de données Amazon Relational Database Service (Amazon RDS) particulier. Cette politique accorde également l'autorisation d'obtenir des informations sur les ElastiCache instantanés Amazon. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	8 septembre 2021
AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications AWS Config de configuration apportées aux nouveaux types de ressources Amazon Elastic Compute Cloud. Pour plus d'informations, consultez Types de ressources pris en charge.	7 septembre 2021

AWS Config prend en charge les nouveaux packs de conformité	Avec cette version, AWS Config met à jour les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour APRA CPG 234 • Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 1 • Meilleures pratiques opérationnelles pour CIS AWS Foundations Benchmark v1.4 niveau 2 • Bonnes pratiques de fonctionnement pour les principes de sécurité du cloud NCSC • Bonnes pratiques de fonctionnement pour NCSC Cyber Assesment Framework • Bonnes pratiques de fonctionnement pour NIST 800 171 • Bonnes pratiques de fonctionnement pour NIST CSF • Bonnes pratiques de fonctionnement pour le cadre de cybersécurité RBI pour les UCB	30 août 2021

- Bonnes pratiques de fonctionnement pour RBI MD-ITF
- Bonnes pratiques de fonctionnement pour NYDFS 23
- Bonnes pratiques de fonctionnement pour PCI DSS 3.2.1

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • aurora-resources-protected-by-backup-plan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-deletion-disabled • backup-recovery-point-minimum-retention-check • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	20 août 2021
AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge le pack de conformité suivant : • Bonnes pratiques de fonctionnement pour NZISM	20 août 2021

Mise à jour de la politique de sécurité Amazon SNS	Avec cette version, AWS Config met à jour la déclaration de politique IAM pour la rubrique Amazon SNS lors de l'utilisation de rôles liés à un service afin d'inclure des protections de sécurité qui limitent l'accès `sourceARN` avec `sourceAccountId` et/ou dans la politique de la rubrique. Elle garantit qu'Amazon SNS accède à vos ressources uniquement pour le compte des utilisateurs et des scénarios attendus. La page suivante est mise à jour : • Autorisations relatives à la rubrique Amazon SNS	17 août 2021

Mise à jour AWS Lambda des politiques de sécurité	Avec cette version, AWS Config met à jour la politique AWS Lambda basée sur les ressources pour les règles AWS Config personnalisées afin d'inclure des protections de sécurité qui limitent l'accès avec `sourceARN` et/ou `sourceAccountId` dans la demande d'appel. Cela permet de AWS Lambda s'assurer que l'accès à vos ressources est réservé aux utilisateurs et aux scénarios attendus. Les pages suivantes sont mises à jour : • AWS::Config::ConfigRule • Élaboration d'une règle personnalisée pour AWS Config	12 août 2021
AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modificat ions AWS Config de configura tion apportées aux types de ressources Amazon Kinesis. Pour plus d'informations, consultez Types de ressource s pris en charge.	6 août 2021

AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge le pack de conformité suivant : • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau élevé) Les packs de conformité suivants sont mis à jour : • Meilleures pratiques opérationnelles pour le pilier de fiabilité du AWS framework Well-Architected • Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau faible) • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau modéré) • Bonnes pratiques de fonctionnement pour la sécurité HIPAA	30 juillet 2021
Exemples de AWS Lambda fonctions pour les règles AWS Config personnalisées	Dans cette version, AWS Config fournit des exemples de fonctions Python dans Example AWS Lambda Functions for AWS Config Rules (Python).	29 juillet 2021

Mise à jour de sécurité IAM	Les politiques `AWSConfigServiceRolePolicy` et `AWS_ConfigRole` accordent désormais des autorisations pour répertorier les balises d'un groupe de journaux, les balises d'une machine d'état et toutes les machines d'état. Ces politiques accordent désormais des autorisations pour obtenir des détails sur une machine d'état. Ces politiques autorisent également désormais des autorisations supplémentaires pour Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming pour Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Simple Notification Service,, SageMaker et. AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	28 juillet 2021

AWS Config prend en charge de nouveaux types de ressources	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configura tion apportées aux types de AWS Backup ressources. Pour plus d'informations, consultez Types de ressources pris en charge.	14 juillet 2021
AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge les packs de conformité suivants : • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG1 • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG2 • Bonnes pratiques de fonctionnement pour les contrôles critiques de sécurité CIS v8 IG3 • Bonnes pratiques de fonctionnement pour NIST 1800 25	9 juillet 2021

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • ssm-document-not-public • s3-account-level-public-access-blocks-periodic	25 juin 2021
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-disabled	10 juin 2021

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais l'autorisation de consulter les autorisations relatives aux AWS Systems Manager documents et aux informations concernant IAM Access Analyzer. Ces politiques prennent désormais en charge AWS des types de ressources supplémentaires pour Amazon Kinesis, Amazon, ElastiCache Amazon EMR, AWS Network Firewall Amazon Route 53 et Amazon Relational Database Service (Amazon RDS). Ces modifications d'autorisation permettent AWS Config d'invoquer les API en lecture seule requises pour prendre en charge ces types de ressources. Ces politiques prennent également désormais en charge le filtrage des fonctions Lambda @Edge pour la règle gérée AWS Config lambda-inside-vpc. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	8 juin 2021

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-enabled • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	19 mai 2021
AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications AWS Config de configuration apportées aux types de ressources Amazon Elastic File System. Pour plus d'informations, consultez Types de ressources pris en charge.	13 mai 2021

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais l'autorisation d' AWS Config effectuer des appels GET en lecture seule à API Gateway afin de prendre en charge une règle de configuration pour API Gateway. Ces politiques ajoutent également des autorisations qui permettent AWS Config d'invoquer les API en lecture seule d'Amazon Simple Storage Service (Amazon S3), qui sont nécessaires pour prendre en charge le nouveau type de ressource. `AWS::S3::AccessPoint` Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	10 mai 2021
AWS Config Règles personnalisées	Les pages suivantes du guide du développeur sont mises à jour : • Commencer à utiliser des règles personnalisées pour AWS Config • Élaboration d'une règle personnalisée pour AWS Config	30 avril 2021

AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade-enabled • redshift-enhanced-vpc-routing-enabled	15 avril 2021

Mise à jour de sécurité IAM	La `AWSConfigServiceRolePolicy` politique et la `AWS_ConfigRole` politique accordent désormais l'autorisation de consulter les informations relatives à des documents AWS Systems Manager spécifiques. Ces politiques prennent également désormais en charge AWS des types de ressources supplémentaires pour AWS Backup Amazon Elastic File System ElastiCache, Amazon, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Kinesis SageMaker, Amazon et Amazon Route 53 AWS Database Migration Service. Ces modifications d'autorisation permettent AWS Config d'invoquer les API en lecture seule requises pour prendre en charge ces types de ressources. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Config.	14 avril 2021

Conformité des packs de conformité en tant qu'éléments de configuration (CI)	Avec cette version, AWS Config prend en charge la conformité des packs de conformité en tant qu'éléments de configuration. Elle vous permet d'effectuer les opérations suivantes : • Afficher une chronologie des modifications apportées à l'état de conformité de vos packs de conformité • Agréger la conformité des packs de conformité sur plusieurs comptes et régions • Utiliser des requêtes avancées pour vérifier la conformité de vos packs de conformité Les types de données suivants sont mis à jour : • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary Les pages suivantes du guide du développeur sont mises à jour : • Affichage des données de conformité dans le tableau	30 mars 2021

	de bord des packs de conformité • Affichage de la chronologie de l'historique de conformité pour les packs de conformité • Affichage des données de conformité dans le tableau de bord Aggregator • Interrogation de l'état de configuration actuel des ressources AWS • Types de ressource pris en charge	
Mise à jour de la pagination	Dans cette version, la fonctionnalité de requêtes AWS Config avancées prend désormais en charge la pagination pour les requêtes contenant des fonctions d'agrégation, telles que COUNT et SUM. Vous pouvez désormais utiliser des requêtes avancées pour obtenir des résultats complets pour vos requêtes agrégées grâce à la pagination, qui étaient auparavant limitées à 500 lignes. Pour plus d'informations, voir Interrogation de l'état de configuration actuel des ressources AWS	26 mars 2021

Prise en charge de la région	Avec cette version, AWS Config and AWS Config Rules est désormais compatible dans la région Asie-Pacifique (Osaka).	4 mars 2021
AWS Config prend en charge de nouveaux types de ressources	Cette version vous permet d'enregistrer les modifications de configuration apportées AWS Config aux types de ressources Amazon Elastic Container Registry, Amazon Elastic Container Service et Amazon Elastic Kubernetes Service. Pour plus d'informa tions, consultez Types de ressources pris en charge.	25 février 2021

Prise en charge du chiffrement KMS	Cette version vous AWS Config permet d'utiliser le chiffrement basé sur le KMS sur les objets fournis par AWS Config pour la livraison du compartiment S3. Les types de données suivants sont mis à jour : • DeliveryChannel • PutDeliveryCanal Les pages suivantes du guide du développeur sont mises à jour : • Autorisations pour la clé KMS • Autorisations pour le rôle IAM attribué à AWS Config	16 février 2021
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	16 février 2021

Prise en charge des régions de requêtes enregistrées	Avec cette version, les requêtes enregistrées sont désormais prises en charge dans les AWS GovCloud régions (USA Est) et AWS GovCloud (USA Ouest).	15 février 2021
Prise en charge de la région d'agrégation des données de plusieurs comptes et plusieurs régions	Dans cette version, l'agrégation de plusieurs comptes et plusieurs régions est désormais prise en charge dans la région Afrique (Le Cap) et Europe (Milan). Pour plus d'informations, consultez Agrégation de données multi-région et multi-compte.	15 février 2021
Requêtes avancées - Prise en charge par région	Dans cette version, les requêtes avancées sont désormais prises en charge dans les régions Afrique (Le Cap) et Europe (Milan). Pour plus d'informations, consultez la section Interrogation de l'état de configuration actuel des AWS ressources.	15 février 2021
AWS Config notification de l'historique de la documentation disponible via le flux RSS	Vous pouvez désormais recevoir des notifications concernant les mises à jour de la AWS Config documentation en vous abonnant à un flux RSS.	1er janvier 2021

Mises à jour antérieures

Le tableau suivant décrit l'historique des publications de documentation AWS Config antérieures au 31 décembre 2020.

Modification	Description	Date de parution
Prise en charge des requêtes enregistrées	Avec cette version, AWS Config vous pouvez enregistrer vos requêtes. Après avoir enregistré la requête, vous pouvez la rechercher, la copier dans l'éditeur de requêtes, la modifier ou la supprimer. Pour plus d'informations sur l'enregistrement des requêtes, consultez Interrogation à l'aide de l'éditeur de requête SQL (console) et Requête à l'aide de l'éditeur de requête SQL (AWS CLI). Pour plus d'informations sur les API, consultez la référence des API AWS Config : • PutStoredRequête • GetStoredRequête • ListStoredRequêtes • DeleteStoredRequête Voir aussi Service Limits.	21 décembre 2020
Prise en charge des vérifications de processus	Cette version AWS Config prend en charge les contrôles de processus , un type de AWS Config règle qui vous permet de suivre vos tâches externes et internes nécessitant une vérification dans le cadre des packs de conformité. Les vérificat	17 décembre 2020

Modification	Description	Date de parution
	ions des processus vous permettent de répertorier la conformité des exigences et des actions en un seul endroit. Pour plus d'informations sur les contrôles de processus, consultez la AWS Config Contrôles de processus dans le cadre d'un pack de conformité rubrique et l'API PutExternald'évaluation.	
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-enabled • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-enabled • rds-cluster-iam-authentication-enabled • redshift-cluster-kms-enabled • s3-bucket-level-public-access-prohibited • subnet-auto-assign-public-ip-disabled • vpc-network-acl-unused-check	17 décembre 2020

Modification	Description	Date de parution
AWS Config soutient AWS Network Firewall	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à vos AWS Network Firewall FirewallPolicy types de ressources et de pare-feu. RuleGroup Pour plus d'informations, consultez Types de ressource pris en charge.	4 décembre 2020
Mise à jour de la documentation	AWS Config ajout de la prise en charge de l'agrégation des données de ressources à l'échelle de l'organisation dans un compte d'administrateur délégué. Vous pouvez désormais utiliser un compte administrateur délégué pour agréger les données de configuration des ressources et de conformité de tous les comptes membres d'une organisation dans AWS Organizations. Pour plus d'informations, consultez PutConfigurationAggregator, Configuration d'un agrégateur à l'aide de la console etEnregistrer un administrateur délégué.	4 décembre 2020

Modification	Description	Date de parution
AWS Config prend en charge les nouveaux packs de conformité	• Bonnes pratiques de fonctionnement pour CMMC niveau 3 • Bonnes pratiques de fonctionnement pour CMMC niveau 4 • Bonnes pratiques de fonctionnement pour CMMC niveau 5 • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau faible) • Bonnes pratiques de fonctionnement pour l'ENS Espagne (niveau modéré) • Bonnes pratiques de fonctionnement pour NCSC Cyber Assesment Framework • Bonnes pratiques de fonctionnement pour le cadre de cybersécurité RBI pour les UCB	30 octobre 2020

Modification	Description	Date de parution
AWS Config prend en charge les nouveaux packs de conformité	• Bonnes pratiques de fonctionnement pour ACSC Essentials 8 • Bonnes pratiques de fonctionnement pour ACSC ISM • Bonnes pratiques de fonctionnement pour l'IA et le ML • Bonnes pratiques de fonctionnement pour la gestion des ressources • Bonnes pratiques de fonctionnement pour le BCP et la DR • Bonnes pratiques de fonctionnement pour EC2 • Bonnes pratiques de fonctionnement pour K-ISMS • Bonnes pratiques de fonctionnement pour l'équilibrage de charge • Bonnes pratiques de fonctionnement pour la journalisation • Bonnes pratiques de fonctionnement pour la surveillance • Bonnes pratiques de fonctionnement pour le sans serveur	22 octobre 2020

Modification	Description	Date de parution
AWS Config prend en charge les nouveaux packs de conformité	• Bonnes pratiques de fonctionnement pour APRA CPG 234 • Bonnes pratiques de fonctionnement pour FedRAMP(Low) • Bonnes pratiques de fonctionnement pour MAS Notice 655 • Bonnes pratiques de fonctionnement pour NBC TRMG • Bonnes pratiques de fonctionnement pour les principes de sécurité du cloud NCSC • Bonnes pratiques de fonctionnement pour RBI MD-ITF	15 octobre 2020

Modification	Description	Date de parution
AWS Config prend en charge les nouveaux packs de conformité	• Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Material • Bonnes pratiques de fonctionnement pour les charges de travail ABS CCIG 2.0 Standard • Bonnes pratiques de fonctionnement pour BNM RMiT • Bonnes pratiques de fonctionnement pour la résilience des données • Bonnes pratiques de fonctionnement pour les services de lac de données et d'analyse • Bonnes pratiques de fonctionnement pour les services de chiffrement et de gestion des clés • Bonnes pratiques de fonctionnement pour la norme FDA CFR Titre 21 Partie 11 • Bonnes pratiques de fonctionnement pour les ressources accessibles au public • Bonnes pratiques de fonctionnement pour MAS TRMG • Bonnes pratiques de fonctionnement pour NERC CIP BCSI • Bonnes pratiques de fonctionnement pour NYDFS 23	8 octobre 2020

Modification	Description	Date de parution
AWS Config prend en charge les nouveaux packs de conformité	• Meilleures pratiques opérationnelles pour le pilier de fiabilité du AWS framework Well-Architected • Meilleures pratiques opérationnelles pour le pilier de sécurité du AWS framework Well-Architected • Bonnes pratiques de fonctionnement pour CMMC niveau 1 • Bonnes pratiques de fonctionnement pour CMMC niveau 2 • Bonnes pratiques de fonctionnement pour les services de calcul • Bonnes pratiques de fonctionnement pour les services de base de données • Bonnes pratiques de fonctionnement pour les services de gestion et de gouvernance • Bonnes pratiques de fonctionnement pour les services de mise en réseau et de diffusion de contenu • Bonnes pratiques de fonctionnement pour les services de sécurité, d'identité et de conformité • Bonnes pratiques de fonctionnement pour les services de stockage	26 octobre 2020

Modification	Description	Date de parution
AWS Config prend en charge les nouveaux packs de conformité	• Bonnes pratiques de fonctionnement pour FedRAMP (modérée) • Bonnes pratiques de fonctionnement pour FFIEC • Bonnes pratiques de fonctionnement pour la sécurité HIPAA • Bonnes pratiques de fonctionnement pour NIST 800-53 rev 4 • Bonnes pratiques de fonctionnement pour NIST 800 171	28 septembre 2020
Mise à jour de la documentation	Les rubriques de pack de conformité suivantes sont mises à jour. • Prérequis • Déploiement d'un pack de conformité à l'aide de la console AWS Config • Gestion des packs de conformité dans tous les comptes de votre organisation	28 septembre 2020
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • iam-customer-policy-blocked-kms-actions • iam-inline-policy-blocked-kms-actions	17 septembre 2020

Modification	Description	Date de parution
AWS Config prend en charge la AWS WAF v2	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à votre WebACL, à votre IPSet et ManagedRuleSet à vos types RegexPatternSet de RuleGroup ressources AWS WAF v2. Pour plus d'informations, consultez Types de ressource pris en charge.	1 septembre 2020
Mise à jour de la documentation	Une note a été ajoutée à Accès complet à AWS Config concernant la création d'autorisations personnalisées qui accordent un accès complet. La documentation a été mise à jour pour les règles suivantes : • s3-bucket-server-side-encryption-enabled • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-platform-check	24 août 2020
Mise à jour de la documentation	Les modèles Bonnes pratiques de fonctionnement pour PCI DSS 3.2.1 et Bonnes pratiques de fonctionnement pour NIST CSF sont mis à jour.	14 août 2020

Modification	Description	Date de parution
Mise à jour de la documentation	Des exemples de requêtes relationnelles sont ajoutés. Pour plus d'informations, consultez Exemples de requêtes relationnelles.	30 juillet 2020
Mise à jour de la documentation	Les types de données suivants sont mis à jour : • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuts • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuts • GetOrganizationConformancePackDetailedStatus	23 juillet 2020
AWS Config prend en charge le type de ressource AWS Systems Manager	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au type de ressource de données du fichier AWS Systems Manager. Pour plus d'informations, consultez Types de ressource pris en charge.	9 juillet 2020

Modification	Description	Date de parution
Mise à jour de la documentation	Les modèles Bonnes pratiques opérationnelles pour la gestion des AWS identités et des accès et Bonnes pratiques de fonctionnement pour PCI DSS 3.2.1 sont mis à jour.	9 juillet 2020

Modification	Description	Date de parution
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • account-part-of-organizations • alb-http-drop-invalid-header-enabled • alb-waf-enabled • cloudfront-default-root-object-configured • cloudfront-origin-access-identity-enabled • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-check • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-access • eks-secrets-encrypted • elasticsearch-node-to-node-encryption-check • elb-cross-zone-load-balancing-enabled • elb-tls-https-listeners-only • iam-no-inline-policy-check	9 juillet 2020

Modification	Description	Date de parution
	• rds-cluster-deletion-protection-enabled • rds-in-backup-plan • rds-instance-deletion-protection-enabled • rds-instance-iam-authentication-enabled • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled Pour plus d'informations, consultez Liste des règles AWS Config gérées.	
Prise en charge de la région d'agrégation des données de plusieurs comptes et plusieurs régions	Dans cette version, l'agrégation de données de plusieurs comptes et plusieurs régions est désormais prise en charge dans les régions Asie-Pacifique (Hong Kong) et Moyen-Orient (Bahreïn). Pour plus d'informations, consultez Multi-Account Multi-Region Data Aggregation et Dépannage pour le regroupement des données de plusieurs comptes et plusieurs régions.	1er juillet 2020

Modification	Description	Date de parution
Requêtes avancées - Prise en charge par région	Dans cette version, les requêtes avancées sont désormais prises en charge dans les régions Asie-Paci fique (Hong Kong) et Moyen-Orient (Bahreïn). Pour plus d'informations, consultez Interrogation de l'état de configuration actuel des ressources AWS.	1er juillet 2020
Mise à jour de la documentation	La documentation a été mise à jour pour les règles suivantes : • ec2-managedinstance-association-compliance-status-check • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3-bucket-policy-grantee-check	30 juin 2020
Mise à jour de la documentation	La documentation a été mise à jour avec des informations sur la sécurité pour AWS Config. veuillez consulter Sécurité dans AWS Config.	24 juin 2020
Mise à jour de la documentation	AWS Control Tower Le modèle du pack de conformité Detective Guardrails est mis à jour. Pour plus d'informations, consultez AWSPack de conformité pour garde-corps Control Tower Detective.	4 juin 2020

Modification	Description	Date de parution
AWS Config prend en charge un nouveau pack de conformité	Cette version AWS Config prend en charge les meilleures pratiques opérationnelles pour le pack de conformité NIST CSF. Pour plus d'informations, consultez Bonnes pratiques de fonctionnement pour NIST CSF .	29 mai 2020
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2-ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3-bucket-default-lock-enabled • s3-default-encryption-kms • securityhub-enabled • sns-encrypted-kms Pour plus d'informations, consultez Liste des règles AWS Config gérées.	28 mai 2020

Modification	Description	Date de parution
Prise en charge de l'adminis trateur délégué	Avec cette version, vous pouvez déployer des AWS Config règles et des packs de conformité à partir de n'importe quel compte de membre délégué de votre organisation, en plus du compte de gestion. Pour plus d'informations sur les API, consultez la référence des API AWS Config : • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuts • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuts • GetOrganizationConformancePackDetailedStatus Pour plus d’informations, consultez Service Limits.	27 mai 2020

Modification	Description	Date de parution
AWS Config règles Support régional	Dans cette version, peu de AWS Config règles sont prises en charge dans les régions d'Afrique (Le Cap) et d'Europe (Milan). Pour obtenir une liste détaillée des règles et des régions dans lesquelles elles sont prises en charge, veuillez consulter Liste des règles AWS Config gérées.	28 avril 2020
AWS Config prend en charge les nouveaux packs de conformité	Cette version AWS Config prend en charge deux packs de conformité. • AWS Pack de conformité pour garde-corps Control Tower Detective • Bonnes pratiques de fonctionn ement pour CIS Pour plus d'informations, consultez Exemples de modèles de pack de conformité.	22 avril 2020
AWS Config prend en charge AWS Secrets Manager	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistr er les modifications de configuration apportées à votre secret Secrets Manager. Pour plus d'informations, consultez Types de ressource pris en charge.	20 avril 2020

Modification	Description	Date de parution
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	16 avril 2020
Prise en charge régionale du pack de conformité	Dans cette version, les packs de conformité sont désormais pris en charge dans les régions Asie-Pacifique (Hong Kong) et Moyen-Orient (Bahreïn). Pour plus d'informations, consultez Conformance Packs.	8 avril 2020
Mise à jour de la documentation	AWS Config les limites sont disponibles dans ce guide du développeur. Pour plus d'informations, consultez Service Limits.	8 avril 2020
Mise à jour de la documentation	Les ressources tierces gérées (c'est-à-dire créées/mises à jour/supprimées) via le AWS CloudFormation registre sont automatiquement suivies en tant qu'éléments de configuration. AWS Config Pour plus d'informations, consultez Enregistrement de configurations pour les ressources tierces.	30 mars 2020

Modification	Description	Date de parution
Mise à jour de la documentation	Les règles AWS Config gérées sont mises à jour pour inclure Région AWS des informations. Pour plus d'informations, consultez Liste des règles AWS Config gérées.	27 mars 2020
AWS Config prend en charge le type de ressource Amazon SNS	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à votre rubrique Amazon SNS. Pour plus d'informations, consultez Types de ressource pris en charge.	6 mars 2020
Prise en charge de la région d'agrégation des données de plusieurs comptes et plusieurs régions	Avec cette version, le regroupement de plusieurs comptes et plusieurs régions est désormais pris en charge dans la région Europe (Stockholm). Pour plus d'informations, consultez Multi-Account Multi-Region Data Aggregation.	5 mars 2020
Requêtes avancées - Prise en charge par région	Avec cette version, les requêtes avancées sont désormais prises en charge dans la Région Europe (Stockholm). Pour plus d'informations, consultez Interrogation de l'état de configuration actuel des ressources AWS.	5 mars 2020

Modification	Description	Date de parution
AWS Config vous permet d'exécuter des requêtes avancées avec des agrégateurs de configuration	Cette version AWS Config ajoute la prise en charge de l'exécution de requêtes avancées basées sur les propriétés de configuration des ressources à l'aide d'agrégateurs de configuration, ce qui vous permet d'exécuter les mêmes requêtes sur plusieurs comptes et régions. Pour plus d'informations, consultez Interrogation de l'état de configuration actuel des ressources AWS. Avec cette version, AWS Config ajoute une `SelectAggregateResourceConfig` API. Pour plus d'informations, consultez SelectAggregateResourceConfigla référence de AWS Config l'API :	28 février 2020
AWS Config prend en charge le type de ressource Amazon SQS	Avec cette version, vous pouvez enregistrer les modifications AWS Config de configuration apportées à votre file d'attente Amazon SQS. Pour plus d'informations, consultez Types de ressource pris en charge.	13 février 2020

Modification	Description	Date de parution
AWS CloudFormation support pour les packs de conformité	Dans cette version, la AWS CloudFormation prise en charge des ressources suivantes a été ajoutée : `AWS::Config::ConformancePack` et `OrganizationConformancePack` . • AWS::Config::ConformancePack Utilisez cette `AWS::Config::ConformancePack` ressource pour créer un pack de conformité qui est un ensemble de AWS Config règles pouvant être facilement déployées dans un compte, une région et au sein de AWS l'organisation. • AWS::Config::OrganizationConformancePack Utilisez la `AWS::Config::OrganizationConformancePack` ressource pour créer un pack de conformité d'organisation contenant des informations sur packs de conformité AWS Config créés dans les comptes des membres.	13 février 2020

Modification	Description	Date de parution
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • api-gw-execution-logging-enabled • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3-account-level-public-access-blocks • sagemaker-endpoint-configuration-kms-key-configured • service-vpc-endpoint-enabled Pour plus d'informations, consultez Liste des règles AWS Config gérées.	20 décembre 2019

Modification	Description	Date de parution
Enregistrement de configurations pour les types de ressources personnalisées	Avec cette version, AWS Config introduit la prise en charge des configurations d'enregistrement pour les types de ressources personnalisés. Vous pouvez publier les données de configuration de ressources tierces, consulter AWS Config et surveiller l'inventaire des ressources et l'historique de configuration à l'aide de AWS Config la console et des API. Pour plus d'informations, consultez Enregistrement de configurations pour les ressources tierces. Pour plus d'informations sur les API, consultez la référence des API AWS Config : • DeleteResourceConfig • PutResourceConfig	20 novembre 2019

Modification	Description	Date de parution
Packs de conformité	Cette version AWS Config introduit des packs de conformité. Les packs de conformité vous permetten t de regrouper un ensemble de AWS Config règles et d'actions correctives qui peuvent ensuite être déployées ensemble en tant qu'entité unique dans l'ensemble de l' AWS organisation. Pour plus d'informa tions, consultez Conformance Packs. Pour plus d'informations sur les API, consultez la référence des API AWS Config : • DeleteOrganizationConforman cePack • DeleteOrganizationConforman cePack • DescribeConformancePacks • DescribeConformancePacks • DescribeConformancePackStatus • DescribeOrganizationConform ancePacks • DescribeOrganizationConform ancePackStatuts • GetConformancePackComplianc eDétails • GetConformancePackComplianc eRésumé • GetOrganizationConformanceP ackDetailedStatus, • PutConformancePack	19 novembre 2019

Modification	Description	Date de parution
	• PutOrganizationConformancePack	
AWS Config prend en charge Amazon OpenSearch Service et les types de AWS Key Managemen t Service ressources	Avec cette version, vous pouvez enregistrer les modifications AWS Config de configuration apportées à votre domaine et à votre AWS Key Management Service clé Amazon OpenSearch Service. Pour plus d'informations, consultez Types de ressource pris en charge.	11 novembre 2019
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-only • kms-cmk-not-scheduled-for-d eletion • sagemaker-notebook-no-direct-internet-access • sagemaker-notebook-instance-kms-key-configured • shield-drt-access Pour plus d'informations, consultez Liste des règles AWS Config gérées.	10 octobre 2019

Modification	Description	Date de parution
AWS Config prend en charge le type de ressource Amazon RDS	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées AWS Config à votre DbCluster et à votre base de données Amazon Relational Database Service (Amazon RDS). ClusterSnapshot Pour plus d'informations, consultez Types de ressource pris en charge.	17 septembre 2019
AWS Config prend en charge le type de ressource Amazon QLDB	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au type de ressource de registre Amazon Quantum Ledger Database (QLDB). Pour plus d'informations, consultez Types de ressource pris en charge.	10 septembre 2019

Modification	Description	Date de parution
AWS Config vous permet d'appliquer une correction automatique aux ressources non conformes telles qu'évaluées par les règles AWS Config	Cette version inclut la prise en charge AWS Config de l'application de mesures de correction automatique à l'aide de documents AWS Systems Manager d'automatisation sur les ressources non conformes, telles qu'évaluées par AWS Config Rules. Pour plus d'informations, consultez Corriger les ressources non conformes à l'aide de règles AWS Config. Avec cette version, les AWS Config nouvelles API suivantes sont ajoutées. Pour en savoir plus, consultez la Référence d'API AWS Config : • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	5 septembre 2019

Modification	Description	Date de parution
AWS Config met à jour les règles gérées	Dans cette version, AWS Config prend en charge les règles gérées suivantes : • alb-http-to-https-redirection-check • api-gw-cache-enabled-and-encrypted • api-gw-endpoint-type-check • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-check • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up Pour plus d'informations, consultez Liste des règles AWS Config gérées.	22 août 2019

Modification	Description	Date de parution
AWS Config met à jour les règles gérées	Avec cette version, AWS Config met à jour les règles gérées suivantes : • cloudfront-viewer-policy-https • ec2-instance-no-public-ip • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-check • vpc-sg-open-only-to-authorized-ports Pour plus d'informations, consultez Liste des règles AWS Config gérées.	31 juillet 2019
AWS Config prend en charge les types de ressources Amazon EC2	Avec cette version, vous pouvez enregistrer les modifications AWS Config de configuration apportées aux ressources Amazon EC2 suivantes : VPCEndpoint, VPC et VPCEndpointService. PeeringConnection Pour plus d'informations, consultez Types de ressource pris en charge.	12 juillet 2019

Modification	Description	Date de parution
AWS Config vous permet de gérer les AWS Config règles dans l'ensemble Comptes AWS d'une organisation	Cette version AWS Config introduit la prise en charge de la gestion des AWS Config règles Comptes AWS dans l'ensemble d'une organisation. Vous pouvez créer, mettre à jour et supprimer des AWS Config règles de manière centralisée pour tous les comptes de votre organisation. Pour plus d'informations, consultez Gestion des AWS Config règles pour tous les comptes de votre organisation. Pour plus d'informations sur les API, consultez la référence des API AWS Config : • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuts • DeleteOrganizationConfigRule	9 juillet 2019

Modification	Description	Date de parution
AWS Config prend en charge les types de ressources Amazon S3 et Amazon EC2	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à la AccountPublicAccessBlock ressource Amazon S3 et aux ressources Amazon EC2 suivantes ; NatGateway EgressOnlyInternetGateway, et. FlowLog Pour plus d'informations, consultez Types de ressource pris en charge.	17 mai 2019
AWS Config met à jour les règles gérées	Avec cette version, AWS Config met à jour les règles gérées suivantes : • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited Pour plus d'informations, consultez Liste des règles AWS Config gérées.	7 mai 2019
AWS Config vous permet de supprimer une action de correction à l'aide AWS Management Console de.	Avec cette version, AWS Config introduit la prise en charge de la suppression d'une action de correction à l'aide AWS Management Console de. Pour plus d'informations, consultez Corriger les ressources non conformes à l'aide de règles AWS Config.	24 avril 2019

Modification	Description	Date de parution
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge une nouvelle règle gérée : fms-shield-resource-policy-check. Pour plus d'informations, consultez Liste des règles AWS Config gérées.	7 avril 2019
AWS Config prend en charge le type de ressource Amazon API Gateway	Avec cette version, vous pouvez enregistrer les AWS Config modificat ions de configuration apportées aux ressources Amazon API Gateway suivantes : Api (WebSocket API), RestApi (API REST), Stage (étape WebSocket API) et Stage (étape API REST). Pour plus d'informations, consultez Types de ressource pris en charge.	20 mars 2019
AWS Config vous permet d'exécuter des requêtes avancées	Cette version AWS Config ajoute la prise en charge de l'exécution de requêtes avancées basées sur les propriétés de configuration des ressources. Pour plus d'informations, consultez Interrogation de l'état de configuration actuel des ressources AWS. Avec cette version, AWS Config ajoute une `SelectResourceConfig` API. Pour plus d'informations, consultez SelectResourceConfig dans le guide de référence de AWS Config l'API :	19 mars 2019

Modification	Description	Date de parution
AWS Config vous permet d'attribuer des balises à vos AWS Config ressources	Avec cette version, AWS Config introduit la prise en charge du contrôle d'accès basé sur des balises pour trois AWS Config ressources : `ConfigRule`, `ConfigurationAggregator`, etAggregationAuthori zation . Pour plus d'informations, consultez Balisage de vos ressource s AWS Config. Dans cette version, vous pouvez ajouter, supprimer ou répertorier des balises à partir de vos ressources AWS Config à l'aide des types de données suivants. Pour en savoir plus, consultez la Référence d'API AWS Config : • ListTagsForResource • TagResource • UntagResource	14 mars 2019

Modification	Description	Date de parution
AWS Config vous permet d'appliquer des mesures correctives aux ressources non conformes telles qu'évaluées par les règles AWS Config	Cette version AWS Config introduit la prise en charge de l'application de mesures correctives à l'aide de documents AWS Systems Manager d'automatisation sur les ressource s non conformes, telles qu'évalué es par AWS Config Rules. Pour plus d'informations, consultez Corriger les ressources non conformes à l'aide de règles AWS Config. Avec cette version, les AWS Config nouvelles API suivantes sont ajoutées. Pour en savoir plus, consultez la Référence d'API AWS Config : • DeleteRemediationConfiguration • DescribeRemediationConfigur ations • DescribeRemediationExecutio nStatus • PutRemediationConfigurations • StartRemediationExécution	12 mars 2019

Modification	Description	Date de parution
AWS Config prend en charge AWS Config les règles de la région de Chine (Ningxia)	Cette version ne prend en charge que 54 AWS Config règles dans la région de Chine (Ningxia). Pour plus d'informations, consultez Liste des règles AWS Config gérées. Toutefois, AWS Config ne prend actuellement pas en charge les règles suivantes dans la région de Chine (Ningxia) : • acm-certificate-expiration-check • cmk-backing-key-rotation-enabled • cloudformation-stack-drift-detection-check • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-check	12 mars 2019

Modification	Description	Date de parution
	• fms-webacl-rulegroup-association-check • guardduty-enabled-centralized • lambda-function-public-access-prohibited • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-p ermissive • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • s3-bucket-server-side-encryption-enabled • s3-bucket-ssl-requests-only	
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les nouvelles règles gérées suivantes : • iam-user-mfa-enabled • s3-bucket-policy-grantee-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	21 janvier 2019

Modification	Description	Date de parution
AWS Config prend en charge le type de ressource Service Catalog	Avec cette version, vous pouvez AWS Config enregistrer les modificat ions de configuration apportées aux ressources Service Catalog suivantes : CloudFromation produit, produit provisionné et portefeuille. Pour plus d'informations, consultez Types de ressource pris en charge.	11 janvier 2019
Support des règles liées aux services AWS Config	Cette version AWS Config ajoute une nouvelle règle de configuration gérée qui permet à d'autres AWS services de créer des AWS Config règles dans votre compte. Pour plus d'informations, consultez Règles liées aux services AWS Config.	20 novembre 2018

Modification	Description	Date de parution
AWS Config vous permet d'agréger les données de configuration des AWS ressources	Avec cette version, AWS Config introduit la prise en charge de l'agrégation des données de configuration des AWS ressources. Pour plus d'informations, consultez Affichage des données de conformité et d'inventaire dans le tableau de bord Agrégateur. Avec cette version, les AWS Config nouvelles API suivantes sont ajoutées. Pour en savoir plus, consultez la Référence d'API AWS Config : • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceComtes • GetAggregateResourceConfig • ListAggregateDiscoveredResources	19 novembre 2018
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les nouvelles règles gérées suivantes : • cloudformation-stack-drift-detection-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	19 novembre 2018

Modification	Description	Date de parution
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les nouvelles règles gérées suivantes : • access-keys-rotated • cloud-trail-cloud-watch-logs-enabled • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • cmk-backing-key-rotation-enabled • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-check • iam-root-access-key-check • iam-user-unused-credentials-check • mfa-enabled-for-iam-console-access • multi-region-cloudtrail-enabled • root-account-hardware-mfa-enabled • vpc-flow-logs-enabled Pour plus d'informations, consultez Liste des règles AWS Config gérées.	12 novembre 2018

Modification	Description	Date de parution
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les nouvelles règles gérées suivantes : • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-check • vpc-default-security-group-closed Pour plus d'informations, consultez Liste des règles AWS Config gérées.	24 octobre 2018
Prise en charge de l'historique de conformité	Cette version prend AWS Config désormais en charge le stockage de l'historique de conformité des ressources tel qu'évalué par AWS Config les règles. Pour plus d'informations, consultez Affichage de la chronologie de l'historique de conformité pour les ressources.	18 octobre 2018
Prise en charge de la région pour le regroupement des données de plusieurs comptes et plusieurs régions	Avec cette version, le regroupement de plusieurs comptes et plusieurs régions est désormais pris en charge dans six nouvelles régions. Pour plus d'informations, consultez Multi-Account Multi-Region Data Aggregation.	4 octobre 2018

Modification	Description	Date de parution
AWS Config prend en charge les autorisations au niveau des ressources pour les actions des API AWS Config Rules	Cette version AWS Config prend en charge les autorisations au niveau des ressources pour certaines actions de l'API AWS Config Rules. Pour plus d'informations sur les API prises en charge, consultez Autorisations prises en charge au niveau des ressources pour les actions d'API de AWS Config règles.	1 octobre 2018
AWS Config prend en charge le type de CodePipeline ressource	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au type de AWS CodePipeline ressource. Pour plus d'informations, consultez Types de ressource pris en charge.	12 septembre 2018

Modification	Description	Date de parution
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les nouvelles règles gérées suivantes : • ec2-instance-managed-by-systems-manager • ec2-managedinstance-association-compliance-status-check • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-permissive Pour plus d'informations, consultez Liste des règles AWS Config gérées.	5 septembre 2018
AWS Config prend en charge le type de ressource AWS Systems Manager	Avec cette version, vous pouvez enregistrer les modifications AWS Config de configuration apportées aux types de ressources de conformité aux correctifs et de conformité des associations de AWS Systems Manager. Pour plus d'informations, consultez Types de ressource pris en charge.	9 août 2018

Modification	Description	Date de parution
AWS Config vous permet de supprimer vos AWS Config données en utilisant AWS Management Console	Avec cette version, AWS Config introduit la prise en charge de l'utilisation de la période de rétention AWS Management Console. Dans le AWS Management Console, vous pouvez sélectionner une période de conservation des données personnalisée pour votre`ConfigurationItems`. Pour plus d'informations, consultez Supprimer des AWS Config données.	7 août 2018
AWS Config prend en charge le type de AWS Shield ressource	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au type de ressource de AWS Shield protection. Pour plus d'informations, consultez Types de ressource pris en charge.	7 août 2018
AWS Config soutient AWS PrivateLink	Avec cette version, des AWS Config supports AWS PrivateLink vous permettent d'acheminer les données entre votre Amazon Virtual Private Cloud (VPC) et l' AWS Config intégralité du réseau. AWS Pour plus d'informations, consultez Utilisation AWS Config avec Interface Amazon VPC Endpoints.	31 juillet 2018

Modification	Description	Date de parution
AWS Config vous permet de supprimer vos AWS Config données	Avec cette version, AWS Config introduit la prise en charge de la période de rétention. AWS Config vous permet de supprimer vos données en spécifiant une période de conservation pour votre`ConfigurationItems`. Pour plus d'informations, consultez Supprimer des AWS Config données. Avec cette version, les AWS Config nouvelles API suivantes sont ajoutées. Pour en savoir plus, consultez la Référence d'API AWS Config : • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	25 mai 2018
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les deux nouvelles règles gérées suivantes : • lambda-function-settings-check • s3-bucket-replication-enabled • iam-policy-blacklisted-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	10 mai 2018

Modification	Description	Date de parution
AWS Config prend en charge le type de AWS X-Ray ressource	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au type de AWS X-Ray EncryptionConfig ressource. Pour plus d'informations, consultez Types de ressource pris en charge.	1 mai 2018
AWS Config prend en charge le type de AWS Lambda ressource et une nouvelle règle gérée	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au type de ressource de AWS Lambda fonction. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend aussi en charge la règle gérée lambda-function-public-access-prohibited. Pour plus d'informations, consultez AWS Config Règles gérées.	25 avril 2018
AWS Config prend en charge le type de AWS Elastic Beanstalk ressource	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées AWS Config aux ressources de l' AWS Elastic Beanstalk application, de la version de l'application et de l'environnement. Pour plus d'informations, consultez Types de ressource pris en charge.	24 avril 2018

Modification	Description	Date de parution
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les deux nouvelles règles gérées suivantes : • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	4 avril 2018

Modification	Description	Date de parution
Regroupement de données multi-comptes et multi-régions	Avec cette version, AWS Config introduit l'agrégation de données multicomptes et multirégions. Cette fonctionnalité vous permet d'agréger AWS Config les données de plusieurs comptes ou d'une organisation et de plusieurs régions dans un compte agrégateur. Pour plus d'informations, consultez Multi-Account Multi-Region Data Aggregation. Avec cette version, les AWS Config nouvelles API suivantes sont ajoutées. Pour en savoir plus, consultez la Référence d'API AWS Config : • PutConfigurationAgrégateur • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAutorisation • DescribeAggregationAutorisations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRègle • DescribeConfigurationAgrégateurs • DescribeConfigurationAggregatorSourcesÉtat	4 avril 2018

Modification	Description	Date de parution
	• DeleteAggregationAutorisation • DeleteConfigurationAgrégateur	
Surveillance AWS Config avec Amazon CloudWatch Events	Dans cette version, utilisez Amazon CloudWatch Events pour détecter et réagir aux changements de statut des AWS Config événements. Pour plus d'informations, consultez Surveillance AWS Config avec Amazon EventBridge.	29 mars 2018
Nouvelle opération d'API	Cette version AWS Config ajoute la prise en charge des BatchGetResourceConfigAPI, vous permettant de récupérer par lots l'état actuel d'une ou de plusieurs de vos ressources.	le 20 mars 2018
AWS Config prend en charge le type de AWS WAF RuleGroup ressource	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées au AWS WAF RuleGroup et aux ressources RuleGroup régionales du AWS WAF. Pour plus d'informations, consultez Types de ressource pris en charge.	15 février 2018

Modification	Description	Date de parution
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les nouvelles règles gérées suivantes : • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl-check • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • iam-group-has-users-check • s3-bucket-server-side-encryption-enabled Pour plus d’informations, consultez Liste des règles AWS Config gérées.	25 janvier 2018
AWS Config prend en charge le type de ressource Elastic Load Balancing	Cette version vous permet d'enregistrer les modifications de configuration apportées AWS Config à vos équilibreurs de charge classiques Elastic Load Balancing. Pour plus d’informations, consultez Types de ressource pris en charge.	17 novembre 2017

Modification	Description	Date de parution
AWS Config prend en charge Amazon CloudFront et le type de AWS WAF ressource	Avec cette version, vous pouvez enregistrer les modifications AWS Config de configuration apportées à votre CloudFront distribution et à votre distribution en streaming. Avec cette version, vous pouvez enregistrer AWS Config les modificat ions de configuration apportées aux ressources suivantes AWS WAF et AWS WAF régionales : règle basée sur le taux, règle et ACL Web. Pour plus d'informations, consultez Types de ressource pris en charge.	15 novembre 2017
AWS Config prend en charge le type de AWS CodeBuild ressource	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistr er les modifications de configuration apportées à vos AWS CodeBuild projets. Pour plus d'informations, consultez Types de ressource pris en charge.	20 octobre 2017

Modification	Description	Date de parution
AWS Config prend en charge les ressources Auto Scaling et une nouvelle règle gérée	Avec cette version, vous pouvez enregistrer les AWS Config modifications de configuration apportées aux ressources Auto Scaling suivantes : groupes, configuration de lancement, actions planifiées et politique de dimensionnement. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend également en charge la règle gérée suivante : • autoscaling-group-elb-healthcheck-required Pour plus d'informations, consultez AWS Config Règles gérées.	18 septembre 2017
AWS Config prend en charge le type de AWS CodeBuild ressource	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à vos AWS CodeBuild projets. Pour plus d'informations, consultez Types de ressource pris en charge.	20 octobre 2017

Modification	Description	Date de parution
AWS Config prend en charge les ressources Auto Scaling et une nouvelle règle gérée	Avec cette version, vous pouvez enregistrer les AWS Config modifications de configuration apportées aux ressources Auto Scaling suivantes : groupes, configuration de lancement, actions planifiées et politique de dimensionnement. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend également en charge la règle gérée suivante : • autoscaling-group-elb-healthcheck-required Pour plus d'informations, consultez AWS Config Règles gérées.	18 septembre 2017
AWS Config prend en charge le type de ressource de table DynamoDB et une nouvelle règle gérée	Avec cette version, vous pouvez enregistrer les modifications AWS Config de configuration apportées à vos tables DynamoDB. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend en charge la règle gérée suivante : • dynamodb-autoscaling-enabled Pour plus d'informations, consultez AWS Config Règles gérées.	8 septembre 2017

Modification	Description	Date de parution
AWS Config prend en charge deux nouvelles règles gérées pour Amazon S3	Cette version prend en charge deux nouvelles règles gérées : • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited Pour plus d'informations, consultez AWS Config Règles gérées.	14 août 2017
Nouvelle page dans la AWS Config console	Vous pouvez utiliser le tableau de bord de la AWS Config console pour voir ce qui suit : • Nombre total de ressources • Nombre total de règles • Nombre de ressources non conformes • Nombre de règles non conformes Pour plus d'informations, consultez Afficher le AWS Config tableau de bord.	17 juillet 2017
Nouvelle opération d'API	Vous pouvez utiliser cette GetDiscoveredResourceCounts AWS Config opération pour renvoyer le nombre de types de ressources, le nombre de chaque type de ressource et le nombre total de ressources enregistrées dans une région pour votre Compte AWS.	17 juillet 2017

Modification	Description	Date de parution
AWS Config prend en charge le type de ressource de AWS CloudFormation pile et une nouvelle règle gérée	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à vos AWS CloudFormation piles. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend en charge la règle gérée suivante : • cloudformation-stack-notification-check Pour plus d'informations, consultez AWS Config Règles gérées.	6 juillet 2017
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge des AWS Config règles de la région du Canada (Centre) et de la région Amérique du Sud (São Paulo). Pour toutes les régions qui prennent en charge les règles de configuration AWS Config et les règles de configuration, voir Régions AWS et Endpoints dans le Références générales AWS.	5 juillet 2017

Modification	Description	Date de parution
Contenu nouveau et mis à jour	AWS Config Les règles sont disponibles dans la AWS GovCloud (US) région. Pour plus d'informations, consultez le Guide de l'utilisateur AWS GovCloud (US). Pour les régions compatibles AWS Config, voir Régions AWS et Endpoints dans le Références générales AWS.	8 juin 2017
AWS Config prend en charge le type de ressource Amazon CloudWatch Alarm et trois nouvelles règles gérées	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration de vos CloudWatch alarmes Amazon. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend en charge trois nouvelles règles gérées : • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check Pour plus d'informations, consultez AWS Config Règles gérées.	1er juin 2017

Modification	Description	Date de parution
Contenu nouveau et mis à jour	Cette version prend en charge la spécification du numéro de version de l'application pour les règles gérées suivantes : • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required Pour plus d'informations, consultez AWS Config Règles gérées.	1er juin 2017
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge des AWS Config règles de la région Asie-Pacifique (Mumbai). Pour plus d'informations, consultez Régions AWS et points de terminaison dans la Références générales AWS.	27 avril 2017

Modification	Description	Date de parution
Contenu nouveau et mis à jour	Cette version prend en charge une expérience de console mise à jour pour l'ajout de règles gérées AWS Config dans votre compte pour la première fois. Lorsque vous configurez AWS Config des règles pour la première fois ou dans une nouvelle région, vous pouvez rechercher des règles AWS gérées par nom, description ou étiquette. Vous pouvez choisir Sélectionner tout pour sélectionner toutes les règles ou bien Effacer tout pour effacer toutes les règles. Pour plus d'informations, consultez Ajout, affichage, mise à jour et suppression de règles (console).	5 avril 2017

Modification	Description	Date de parution
AWS Config prend en charge les nouvelles règles gérées	Cette version prend en charge les nouvelles règles gérées suivantes : • acm-certificate-expiration-check • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-inventory-blacklisted • ec2-volume-inuse-check • iam-user-group-membership-check • iam-user-no-policies-check • s3-bucket-ssl-requests-only Pour plus d'informations, consultez Liste des règles AWS Config gérées.	21 février 2017
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge AWS Config des règles dans la région Europe (Londres). Pour plus d'informations, consultez Régions AWS et points de terminaison dans la Références générales AWS.	21 février 2017
Contenu nouveau et mis à jour	Cette version ajoute AWS CloudFormation des modèles pour les règles AWS Config gérées. Vous pouvez utiliser les modèles pour créer des règles gérées pour votre compte. Pour plus d'informations, consultez Création de règles gérées AWS Config avec des modèles AWS CloudFormation.	16 février 2017

Modification	Description	Date de parution
Contenu nouveau et mis à jour	Cette version prend désormais en charge un nouveau mode de test pour l'API `PutEvaluations` . Définissez le paramètre `TestMode` sur true dans votre règle personnal isée pour vérifier si votre fonction AWS Lambda envoie des résultats d'évaluation à AWS Config. Aucune mise à jour n'a lieu sur vos évaluatio ns existantes, et les résultats d'évaluation ne sont pas envoyés à AWS Config. Pour plus d'informations, consultez PutEvaluationsla référence de AWS Config l'API.	16 février 2017
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge des AWS Config règles dans les régions Asie-Pacifique (Séoul) et USA Ouest (Californie du Nord). Pour plus d'informations, consultez Régions AWS et points de terminais on dans la Références générales AWS.	21 décembre 2016
Contenu nouveau et mis à jour	Cette version ajoute la prise AWS Config en charge de la région Europe (Londres). Pour plus d'informations, consultez Régions AWS et points de terminaison dans la Références générales AWS.	13 décembre 2016

Modification	Description	Date de parution
Contenu nouveau et mis à jour	Cette version ajoute la prise AWS Config en charge de la région du Canada (Centre). Pour plus d'informations, consultez Régions AWS et points de terminaison dans la Références générales AWS.	8 décembre 2016
AWS Config prend en charge les types de ressources Amazon Redshift et deux nouvelles règles gérées	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées AWS Config à vos clusters Amazon Redshift, à vos groupes de paramètres de cluster, à vos groupes de sécurité de cluster, à vos instantanés de cluster, à vos groupes de sous-réseaux de clusters et à vos abonnements à des événements. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend en charge deux nouvelles règles gérées : • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	7 décembre 2016

Modification	Description	Date de parution
Contenu nouveau et mis à jour	Cette version prend en charge une nouvelle règle gérée : • dynamodb-throughput-limit-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	7 décembre 2016
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge de la création de 50 règles maximum par région dans un compte. Pour plus d'informations, consultez Limites de configuration AWS dans la Références générales AWS.	7 décembre 2016

Modification	Description	Date de parution
AWS Config prend en charge le type de ressource d'inventaire des instances gérées pour Amazon EC2 Systems Manager et trois nouvelles règles gérées	Avec cette version, vous pouvez enregistrer les modifications AWS Config de configuration logicielle sur vos instances gérées avec la prise en charge de l'inventaire des instances gérées. Pour plus d'informations, consultez Recording Software Configuration for Managed Instances. Cette version prend en charge trois nouvelles règles gérées : • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applications-required • ec2-managedinstance-platform-check Pour plus d'informations, consultez Liste des règles AWS Config gérées.	1 décembre 2016

Modification	Description	Date de parution
AWS Config prend en charge la ressource du compartiment Amazon S3 et deux nouvelles règles gérées	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistrer les modifications de configuration apportées à vos compartiments Amazon S3. Pour plus d'informations, consultez Types de ressource pris en charge. Cette version prend en charge deux nouvelles règles gérées : • s3-bucket-logging-enabled • s3-bucket-versioning-enabled Pour plus d'informations, consultez AWS Config Règles gérées.	18 octobre 2016
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge AWS Config et AWS Config les règles de la région USA Est (Ohio). Pour plus d'informations, consultez Régions AWS et points de terminaison dans la Références générales AWS.	17 octobre 2016

Modification	Description	Date de parution
Règles gérées nouvelles et mises à jour	Cette mise à jour ajoute la prise en charge de huit nouvelles règles gérées : • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted Vous pouvez spécifier plusieurs valeurs de paramètre pour les règles suivantes : • desired-instance-tenancy • required-tags Pour plus d'informations, consultez Liste des règles AWS Config gérées.	4 octobre 2016

Modification	Description	Date de parution
Contenu nouveau et mis à jour pour la AWS Config console	Cette mise à jour ajoute la prise en charge de AWS CloudTrail l'affichage de l'activité des API dans la AWS Config chronologie. Si CloudTrail vous vous connectez pour votre compte, vous pouvez consulter les événements de création, de mise à jour et de suppression d'API pour les modifications de configuration de vos ressources. Pour plus d'informations, consultez Affichage de l'historique de configuration et de conformité.	06 septembre 2016
AWS Config prend en charge le type de ressource Elastic Load Balancing	Cette version vous permet d'enregistrer les modifications de configuration apportées AWS Config aux équilibreurs de charge de votre application Elastic Load Balancing. Pour plus d'informations, consultez Types de ressource pris en charge.	31 août 2016
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge des AWS Config règles dans les régions Asie-Pacifique (Singapour) et Asie-Pacifique (Sydney). Pour plus d'informations, consultez Régions AWS et points de terminaison dans la Références générales AWS.	le 18 août 2016

Modification	Description	Date de parution
Contenu nouveau et mis à jour pour les AWS Config règles	Cette mise à jour ajoute la prise en charge de la création d'une règle qui peut être déclenchée par des changements de configuration et à une fréquence périodique que vous choisissez. Pour plus d'informations, consultez Mode d'évaluation et types de déclencheurs pour les AWS Config règles. Cette mise à jour ajoute également la prise en charge de l'évaluation manuelle de vos ressources par rapport à votre règle et de la suppression des résultats de l'évaluation. Pour plus d'informations, consultez Évaluer vos ressources à l'aide de AWS Config règles. Cette mise à jour ajoute également la prise en charge de l'évaluation des types de ressources supplémentaires à l'aide de règles personnalisées. Pour plus d'informations, consultez Évaluation des types de ressources supplémentaires.	25 juillet 2016

Modification	Description	Date de parution
AWS Config prend en charge les types de ressources Amazon RDS et AWS Certificate Manager (ACM)	Avec cette version, vous pouvez enregistrer les modifications de configuration apportées AWS Config à vos instances de base de données Amazon Relational Database Service (Amazon RDS), à vos groupes de sécurité de base de données, à vos instantanés de base de données, à vos groupes de sous-réseaux de base de données et à vos abonnements aux événements. Vous pouvez également l'utiliser AWS Config pour enregistrer les modificat ions de configuration apportées aux certificats fournis par ACM. Pour plus d'informations, consultez Types de ressource pris en charge.	21 juillet 2016
Informations mises à jour sur la gestion de l'enregistreur de configuration	Cette mise à jour ajoute des étapes pour renommer et supprimer l'enregis treur de configuration à Gestion de l'enregistreur de configuration.	07 juillet 2016

Modification	Description	Date de parution
Création de rôle simplifiée et stratégies mises à jour	Avec cette mise à jour, la création d'un rôle IAM pour AWS Config est simplifiée. Cette amélioration est disponible dans les régions qui prennent en charge les règles de configuration. Pour prendre en charge cette amélioration, les étapes de Configuration à l' AWS Config aide de la console sont mises à jour, l'exemple de stratégie de Autorisations pour le compartiment Amazon S3 pour le canal AWS Config de diffusion est mis à jour et l'exemple de stratégie de Exemples de politiques basées sur l'identité pour AWS Config est mis à jour.	31 mars 2016
Exemples de fonctions et d'événements pour les règles de configuration	Cette mise à jour fournit des exemples de fonctions mis à jour dans Exemples de AWS Lambda fonctions pour AWS Config les règles (Node.js) et cette mise à jour ajoute des exemples d'événements dans Exemple d'événements pour les règles d' AWS Config.	29 mars 2016
AWS Config GitHub Référentiel de règles	Cette mise à jour ajoute des informations sur le GitHub référentiel de AWS Config règles àÉvaluation des ressources à l'aide de AWS Config règles. Ce référentiel fournit des exemples de fonctions pour les règles personnalisées développées et mises à disposition par AWS Config les utilisateurs.	1 mars 2016

Modification	Description	Date de parution
AWS Config Règles	Cette version introduit AWS Config des règles. Les règles vous permettent d' AWS Config évaluer si vos AWS ressources sont conformes aux configurations souhaitées. Pour plus d'informations, consultez Évaluation des ressources à l'aide de AWS Config règles.	18 décembre 2015
AWS Config prend en charge les types de ressources IAM	Avec cette version, vous pouvez enregistrer les AWS Config modificat ions de configuration apportées à vos utilisateurs, groupes, rôles et politiques gérées par le client IAM. Pour plus d'informations, consultez Types de ressource pris en charge.	10 décembre 2015
AWS Config prend en charge l'hôte dédié EC2	Avec cette version, vous pouvez l'utiliser AWS Config pour enregistr er les modifications de configuration de vos hôtes dédiés EC2. Pour plus d'informations, consultez Types de ressource pris en charge.	23 novembre 2015

Modification	Description	Date de parution
Informations mises à jour sur les autorisations	Cette mise à jour ajoute des informations sur les politiques AWS gérées suivantes pour AWS Config : • `AWS_ConfigRole` : accorde à AWS Config l'autorisation d'obtenir des détails de configuration sur vos ressources. Pour plus d'informations, consultez Politique de rôle IAM pour obtenir des détails de configuration. • `AWSConfigUserAccess` — Accorde un accès en lecture seule à un AWS Config utilisateur. Pour plus d'informations, consultez Accès en lecture seule à AWS Config.	19 octobre 2015
AWS Config Aperçu des règles	Cette version introduit l'aperçu AWS Config des règles. Les règles vous permettent d' AWS Config évaluer si vos AWS ressources sont conformes aux configurations souhaitées. Pour plus d'informations, consultez Évaluation des ressources à l'aide de AWS Config règles.	7 octobre 2015
Contenu nouveau et mis à jour	Cette version ajoute la possibilité de rechercher les AWS Config ressources découvertes. Pour plus d'informations, consultez Recherche de ressources découvertes par AWS Config.	27 août 2015

Modification	Description	Date de parution
Contenu nouveau et mis à jour	Cette version ajoute la possibilité de choisir les types de ressource qu' AWS Config enregistre. Pour plus d'informations, consultez AWS Ressources d'enregistrement.	23 juin 2015
Contenu nouveau et mis à jour	Cette version ajoute la prise en charge dans les régions suivantes : Asie-Pacifique (Tokyo), Asie-Pacifique (Singapour), Europe (Francfort), Amérique du Sud (São Paulo) et USA Ouest (Californie du Nord). Pour plus d'informations, consultez Régions AWS and Endpoints.	6 avril 2015
Nouveau guide	Cette version présente AWS Config.	12 novembre 2014

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.